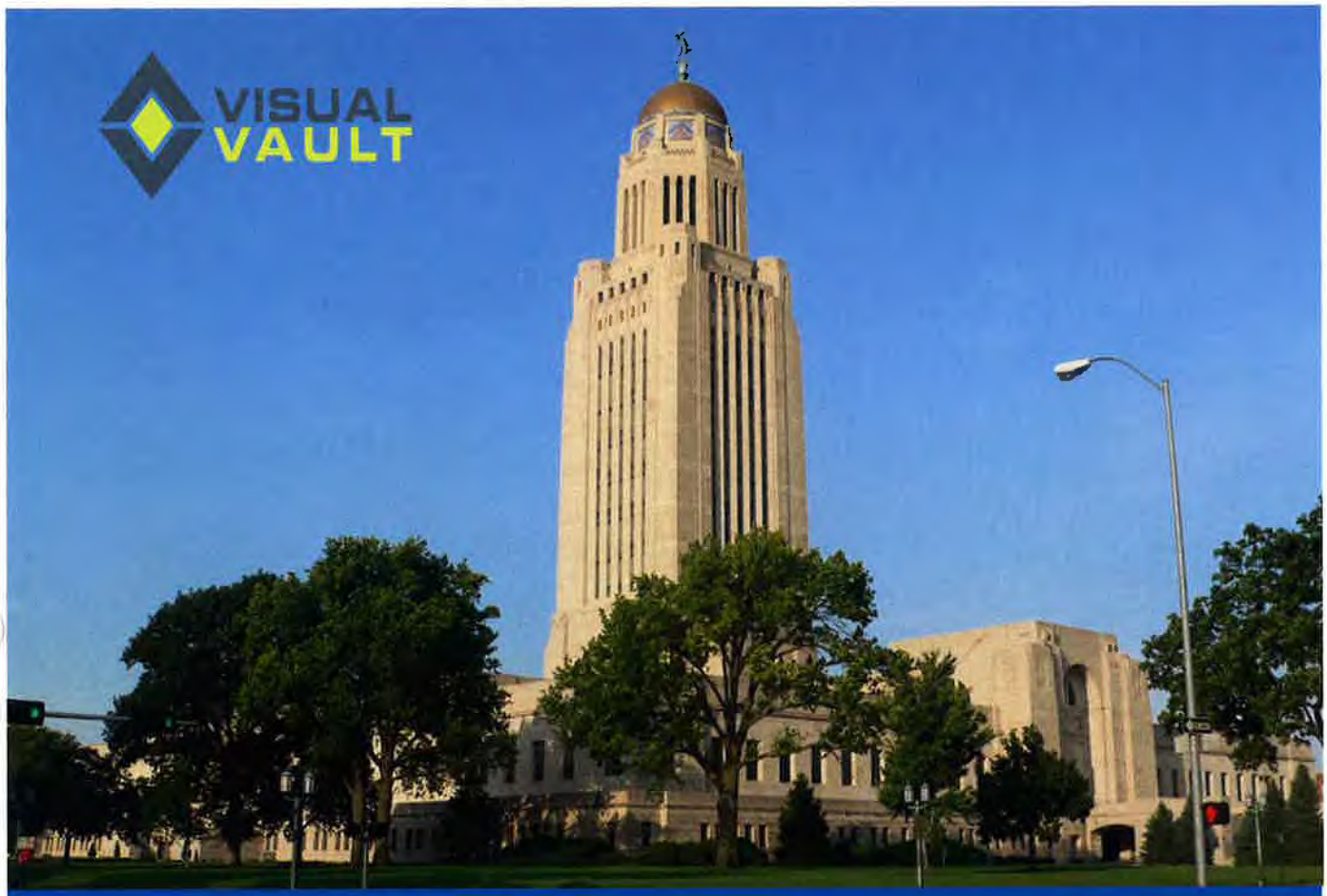
NEBRASKA

Good Life. Great Mission.

DEPT. OF HEALTH AND HUMAN SERVICES



RFP: 5948 Z1
Nebraska DHHS Aging Information Management System

TECHNICAL RESPONSE
VISUALVAULT

PREPARED FOR:
Nancy Storant / Annette Walton, State Purchasing Bureau – 1526 K St. Suite 130 Lincoln, NE. 68508
Phone 402.471.6500 email as.materielpurchasing@nebraska.gov

PRESENTED BY:
Steve Pendelton VisualVault Managing Director, Public Sector
steve.pendelton@visualvault.com
O: 207.536.5854 C: 847.722.7023 2050 E. ASU Circle Suite 103 Tempe, AZ 85284
www.visualvault.com

Technical Proposal

Table of Contents
RFP 5948 Z1

TAB 4

Technical and Audit Documentation

Attachment A GRM VisualVault 2016 Type 2 SOA 2 Final Report
Attachment A3 - GRM VisualVault 2018 Type 1 HIPAA Final Report
Attachment A4 - VisualVault Section 508 VPAT
Attachment B GRM VisualVault HIPAA-HITECH Security Assessment - Final Report
Attachment C GRM VisualVault Support for HIPAA Compliance
Attachment D - GRM VisualVault Technical Summary
Attachment F - GRM VisualVault Disaster Recover and Business Continuity Plan (ISO-0015)
Attachment G - GRM VisualVault Network Architecture (redacted)
Attachment H GRM VisualVault IT Security Standard (STD-0001)
Attachment J GRM VisualVault Software Development Life Cycle (SOP-006)
Attachment K1 Project Management and Testing Methodologies
Attachment K2 Change Control
Attachment L GRM VisualVault data Retention Backup and Restore (SPO-009)
Attachment P GRM VisualVault Encryption and Key Management
Attachment Q GRM VisualVault Information Security Incident Management (ISO-0039)
Attachment R GRM VisualVault Information Security Incident Response Plan (ISO-0040 redacted)
Attachment P - GRM VisualVault Encryption and Key Management

TAB 1

TAB 1

REQUEST FOR PROPOSAL FORM

REQUEST FOR PROPOSAL FORM

NEBRASKA
Good Life. Great Mission.
DEPT. OF HEALTH AND HUMAN SERVICES
• Create the New Normal • Transform Service • Transform Outcomes

BIDDER MUST COMPLETE THE FOLLOWING.....

By signing this Request for Proposal for Contractual Services form, the bidder guarantees compliance with the procedures stated in this Request for Proposal, and agrees to the terms and conditions unless otherwise indicated in writing and certifies that bidder maintains a drug free work place.

Per Nebraska's Transparency in Government Procurement Act, Neb. Rev Stat § 73-603 DAS is required to collect statistical information regarding the number of contracts awarded to Nebraska Contractors. This information is for statistical purposes only and will not be considered for contract award purposes.

_____ NEBRASKA CONTRACTOR AFFIDAVIT: Bidder hereby attests that bidder is a Nebraska Contractor. "Nebraska Contractor" shall mean any bidder who has maintained a bona fide place of business and at least one employee within this state for at least the six (6) months immediately preceding the posting date of this RFP.

_____I hereby certify that I am a Resident disabled veteran or business located in a designated enterprise zone in accordance with Neb. Rev. Stat. § 73-107 and wish to have preference, if applicable, considered in the award of this contract.

_____ I hereby certify that I am a blind person licensed by the Commission for the Blind & Visually Impaired in accordance with Neb. Rev. Stat. §71-8611 and wish to have preference considered in the award of this contract.

FORM MUST BE SIGNED USING AN INDELIBLE METHOD (NOT ELECTRONICALLY)

FIRM:	VisualVault / GRM Information Management Systems, Inc.
COMPLETE ADDRESS:	2050 E. ASU Circle Suite 103 Tempe, Arizona 85284
TELEPHONE NUMBER:	480-308-4400
FAX NUMBER:	N/A
DATE:	November ~~19~~ 30, 2018
SIGNATURE:	
TYPED NAME & TITLE OF SIGNER:	Tod S. Olsen

FORM A - VISUALVAULT BIDDER CONTACT SHEET

Request for Proposal Number 5948 Z1

Form A should be completed and submitted with each response to this RFP. This is intended to provide the State with information on the bidder's name and address, and the specific person(s) who are responsible for preparation of the bidder's response.

Preparation of Response Contact Information	
Bidder Name:	VisualVault / GRM Information Management Systems, Inc.
Bidder Address:	2050 E. ASU Circle Suite 103 Tempe, Arizona 85284
Contact Person & Title:	Steve Pendleton, Managing Director - Public Sector
E-mail Address:	Steve.pendleton@visualvault.com
Telephone Number (Office):	207.536.5854 Office
Telephone Number (Cellular):	847.722.7023 Mobile
Fax Number:	N/A

Each bidder should also designate a specific contact person who will be responsible for responding to the State if any clarifications of the bidder's response should become necessary. This will also be the person who the State contacts to set up a presentation/demonstration, if required.

Communication with the State Contact Information	
Bidder Name:	VisualVault / GRM Information Management Systems, Inc.
Bidder Address:	2050 E. ASU Circle Suite 103 Tempe, Arizona 85284
Contact Person & Title:	Steve Pendleton, Managing Director - Public Sector
E-mail Address:	Steve.pendleton@visualvault.com
Telephone Number (Office):	207.536.5854 Office
Telephone Number (Cellular):	847.722.7023 Mobile
Fax Number:	N/A

TAB 2

TAB 2

CORPORATE OVERVIEW

CORPORATE OVERVIEW

BIDDER IDENTIFICATION AND INFORMATION

The bidder should provide the full company or corporate name, address of the company's headquarters, entity organization (corporation, partnership, proprietorship), state in which the bidder is incorporated or otherwise organized to do business, year in which the bidder firm is organized to do business and whether the name and form of organization has been the same since first organized.

VisualVault is creating a New Normal for states delivering life critical services to NE's aging population. NE DHHS' new service levels, outcomes, and reporting will become the new normal and a bench mark for other departments to emulate

Company name:	GRM Information Management Systems, Inc. / VisualVault (No name or form change since first organized.)
Ownership (sole proprietor, partnership, etc.):	S Corporation
State of incorporation:	New Jersey
Date of incorporation:	1986
# of years in business:	32
List of top officers:	President - Moishe Mana Officer - Jerry Glatt
Location of company headquarters, including City and State:	215 Coles St. Jersey City, NJ 07310
Location(s) of the office that shall provide the services described in this RFP:	2050 E. ASU Circle Suite 103 Tempe, AZ 85284
Number of employees locally with the expertise to support the requirements identified in this RFP:	0
Number of employees nationally with the expertise to support the requirements in this RFP:	200+
Location(s) from which employees shall be assigned for this project:	2050 E. ASU Circle Suite 103 Tempe, AZ 85284

FINANCIAL STATEMENTS

The bidder should provide financial statements applicable to the firm. If publicly held, the bidder should provide a copy of the corporation's most recent audited financial reports and statements, and the name, address, and telephone number of the fiscally responsible representative of the bidder's financial or banking organization.

If the bidder is not a publicly held corporation, either the reports and statements required of a publicly held corporation, or a description of the organization, including size, longevity, client base, areas of specialization and expertise, and any other pertinent information, should be submitted in such a manner that proposal evaluators may reasonably formulate a determination about the stability and financial strength of the organization. Additionally, a non-publicly held firm should provide a banking reference.

The bidder must disclose any and all judgments, pending or expected litigation, or other real or potential financial reversals, which might materially affect the viability or stability of the organization, or state that no such condition is known to exist.

The State may elect to use a third party to conduct credit checks as part of the corporate overview evaluation.

Please see **Attachment 1 Financial Statements** at the end of **TAB 2** of this proposal for our most recent financial statement. VisualVault has no judgments, pending or expected litigation, or other real or potential financial reversals which might materially affect the viability or stability of the organization to report. VisualVault agrees to allow The State to use a third party to conduct credit checks as part of the corporate overview evaluation.

CHANGE OWNERSHIP

If any change in ownership or control of the company is anticipated during the twelve (12) months following the proposal due date the bidder should describe the circumstances of such change and indicate when the change will likely occur. Any change of ownership to an awarded vendor(s) will require notification to the State.

N/A - No change in ownership.

OFFICE LOCATION

The bidder's office location responsible for performance pursuant to an award in connection with the State of Nebraska should be identified.

VisualVault
2050 E. ASU Circle
Suite 103
Tempe, AZ 85284

RELATIONSHIPS WITH STATE

The bidder should describe any dealings with the State over the previous ten (10) years. If the organization, its predecessor, or any Party named in the bidder's proposal response has contracted with the State, the bidder should identify the contract number(s) and/or any other information available to identify such contract(s). If no such contracts exist, so declare.

N/A - No relationship with State.

BIDDER'S EMPLOYEE RELATIONS TO STATE

If any Party named in the bidder's proposal response is or was an employee of the State within the past twenty-four (24) months, identify the individual(s) by name, State agency with whom employed, job title or position held with the State, and separation date. If no such relationship exists or has existed, so declare.

If any employee of any agency of the State of Nebraska is employed by the bidder or is a Subcontractor to the bidder, as of the due date for proposal submission, identify all such persons by name, position held with the bidder, and position held with the State (including job title and agency). Describe the responsibilities of such persons within the proposing organization. If, after review of this information by the State, it is determined that a conflict of interest exists or may exist, the bidder may be disqualified from further consideration in this proposal. If no such relationship exists, so declare.

N/A - No employee relations to State.

CONTRACT PERFORMANCE

If the bidder or any proposed subcontractor has had a contract terminated for default during the past ten (10) years, all such instances must be described as required below. Termination for default is defined as a notice to stop performance delivery due to the bidder's non-performance or poor performance, and the issue was either not litigated due to inaction on the part of the bidder or litigated and such litigation determined the bidder to be in default.

It is mandatory that the bidder submit full details of all termination for default experienced during the past ten (10) years, including the other Party's name, address, and telephone number. The response to this section must present the bidder's position on the matter. The State will evaluate the facts and will score the bidder's proposal accordingly. If no such termination for default has been experienced by the bidder in the past ten (10) years, so declare.

If at any time during the past ten (10) years, the bidder has had a contract terminated for convenience, non-performance, non-allocation of funds, or any other reason, describe fully all circumstances surrounding such termination, including the name and address of the other contracting Party.

N/A - No terminated contracts.

ADDENDUM ACKNOWLEDGMENT

VisualVault acknowledges the following:

Addendum #1 Revised Schedule of Events - posted 11/14/18

Addendum #2 Questions and Answers - posted 11/15/18

TERMS AND CONDITIONS

Bidders should complete Sections II through VII as part of their proposal. Bidder is expected to read the Terms and Conditions and should initial either accept, reject, or reject and provide alternative language for each clause. The bidder should also provide an explanation of why the bidder rejected the clause or rejected the clause and provided alternate language. By signing the RFP, bidder is agreeing to be legally bound by all the accepted terms and conditions, and any proposed alternative terms and conditions submitted with the proposal. The State reserves the right to negotiate rejected or proposed alternative language. If the State and bidder fail to agree on the final Terms and Conditions, the State reserves the right to reject the proposal. The State of Nebraska is soliciting proposals in response to this RFP. The State of Nebraska reserves the right to reject proposals that attempt to substitute the bidder's commercial contracts and/or documents for this RFP.

Please see executed Terms and Conditions, next page.

Remainder of page intentionally left blank.

TERMS AND CONDITIONS
RFP NUMBER 5948 Z1
VISUALVAULT RESPONSE

The bidders should submit with their proposal any license, user agreement, service level agreement, or similar documents that the bidder wants incorporated in the Contract. The State will not consider incorporation of any document not submitted with the bidder's proposal as the document will not have been included in the evaluation process. These documents shall be subject to negotiation and will be incorporated as addendums if agreed to by the Parties.

Please see Attachment 2 for the following exhibits included at the end of TAB 2 of this proposal.

Exhibit A - Hosting Agreement
Exhibit B - Acceptable Use Policy
Exhibit C - Support SLAs

If a conflict or ambiguity arises after the Addendum to Contract Award have been negotiated and agreed to, the Addendum to Contract Award shall be interpreted as follows:

1. If only one Party has a particular clause then that clause shall control;
2. If both Parties have a similar clause, but the clauses do not conflict, the clauses shall be read together;
3. If both Parties have a similar clause, but the clauses conflict, the State's clause shall control.

A. GENERAL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The contract resulting from this RFP shall incorporate the following documents:

1. Request for Proposal and Addenda;
2. Amendments to the RFP;
3. Questions and Answers;
4. Contractor's proposal (RFP and properly submitted documents);
5. The executed Contract and Addendum One to Contract, if applicable; and,
6. Amendments/Addendums to the Contract.

These documents constitute the entirety of the contract.

Unless otherwise specifically stated in a future contract amendment, in case of any conflict between the incorporated documents, the documents shall govern in the following order of preference with number one (1) receiving preference over all other documents and with each lower numbered document having preference over any higher numbered document: 1) Amendment to the executed Contract with the most recent dated amendment having the highest priority, 2) executed Contract and any attached Addenda, 3) Amendments to RFP and any Questions and Answers, 4) the original RFP document and any Addenda, and 5) the Contractor's submitted Proposal.

Any ambiguity or conflict in the contract discovered after its execution, not otherwise addressed herein, shall be resolved in accordance with the rules of contract interpretation as established in the State of Nebraska.

B. NOTIFICATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

Contractor and State shall identify the contract manager who shall serve as the point of contact for the executed contract.

Communications regarding the executed contract shall be in writing and shall be deemed to have been given if delivered personally or mailed, by U.S. Mail, postage prepaid, return receipt requested, to the parties at their respective addresses set forth below, or at such other addresses as may be specified in writing by either of the parties. All notices, requests, or communications shall be deemed effective upon personal delivery or three (3) calendar days following deposit in the mail.

Vendor Contract Manager	Tod S. Olsen
Vendor	VisualVault
Vendor Street Address	2050 E. ASU Circle Suite 103
Vendor City, State, Zip	Tempe, AZ 85284

C. GOVERNING LAW (Statutory)

Notwithstanding any other provision of this contract, or any amendment or addendum(s) entered into contemporaneously or at a later time, the parties understand and agree that, (1) the State of Nebraska is a sovereign state and its authority to contract is therefore subject to limitation by the State's Constitution, statutes, common law, and regulation; (2) this contract will be interpreted and enforced under the laws of the State of Nebraska; (3) any action to enforce the provisions of this agreement must be brought in the State of Nebraska per state law; (4) the person signing this contract on behalf of the State of Nebraska does not have the authority to waive the State's sovereign immunity, statutes, common law, or regulations; (5) the indemnity, limitation of liability, remedy, and other similar provisions of the final contract, if any, are entered into subject to the State's Constitution, statutes, common law, regulations, and sovereign immunity; and, (6) all terms and conditions of the final contract, including but not limited to the clauses concerning third party use, licenses, warranties, limitations of liability, governing law and venue, usage verification, indemnity, liability, remedy or other similar provisions of the final contract are entered into specifically subject to the State's Constitution, statutes, common law, regulations, and sovereign immunity.

The Parties must comply with all applicable local, state and federal laws, ordinances, rules, orders, and regulations.

D. BEGINNING OF WORK

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The bidder shall not commence any billable work until a valid contract has been fully executed by the State and the successful Contractor. The Contractor will be notified in writing when work may begin.

E. CHANGE ORDERS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The State and the Contractor, upon the written agreement, may make changes to the contract within the general scope of the RFP. Changes may involve specifications, the quantity of work, or such other items as the State may find necessary or desirable. Corrections of any deliverable, service, or work required pursuant to the contract shall not be deemed a change. The Contractor may not claim forfeiture of the contract by reasons of such changes.

For all changes, the Contractor shall follow the Change Control Plan set forth in Section V.1.d.v. Any in-scope changes will require a written change order that will generate an Amendment to the contract. Changes in work and the amount of compensation to be paid to the Contractor shall be determined in accordance with applicable unit prices if any, a pro-rated value, or through negotiations. The State shall not incur a price increase for changes that should have been included in the Contractor's proposal, were foreseeable, or result from difficulties with or failure of the Contractor's proposal or performance.

No change shall be implemented by the Contractor until approved by the State, and the Contract is amended to reflect the change and associated costs, if any. If there is a dispute regarding the cost, but both parties agree that immediate implementation is necessary, the change may be implemented, and cost negotiations may continue with both Parties retaining all remedies under the contract and law.

F. NOTICE OF POTENTIAL CONTRACTOR BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

If Contractor breaches the contract or anticipates breaching the contract, the Contractor shall immediately give written notice to the State. The notice shall explain the breach or potential breach, a proposed cure, and may include a request for a waiver of the breach if so desired. The State may, in its discretion, temporarily or permanently waive the breach. By granting a waiver, the State does not forfeit any rights or remedies to which the State is entitled by law or equity, or pursuant to the provisions of the contract. Failure to give immediate notice, however, may be grounds for denial of any request for a waiver of a breach.

G. BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

Either Party may terminate the contract, in whole or in part, if the other Party breaches its duty to perform its

'gations under the contract in a timely and proper manner. Termination requires written notice of default and a .ty (30) calendar day (or longer at the non-breaching Party's discretion considering the gravity and nature of the default) cure period. Said notice shall be delivered by Certified Mail, Return Receipt Requested, or in person with proof of delivery. Allowing time to cure a failure or breach of contract does not waive the right to immediately terminate the contract for the same or different contract breach which may occur at a different time. In case of default of the Contractor, the State may contract the service from other sources and hold the Contractor responsible for any excess cost occasioned thereby

The State's failure to make payment shall not be a breach, and the Contractor shall retain all available statutory remedies and protections.

H. NON-WAIVER OF BREACH

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The acceptance of late performance with or without objection or reservation by a Party shall not waive any rights of the Party nor constitute a waiver of the requirement of timely performance of any obligations remaining to be performed.

I. SEVERABILITY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

If any term or condition of the contract is declared by a court of competent jurisdiction to be illegal or in conflict with any law, the validity of the remaining terms and conditions shall not be affected, and the rights and obligations of the parties shall be construed and enforced as if the contract did not contain the provision held to be invalid or illegal.

J. INDEMNIFICATION

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

1. GENERAL

The Contractor agrees to defend, indemnify, and hold harmless the State and its employees, volunteers, agents, and its elected and appointed officials ("the indemnified parties") from and against any and all third party claims, liens, demands, damages, liability, actions, causes of action, losses, judgments, costs, and expenses of every nature, including investigation costs and

expenses, settlement costs, and attorney fees and expenses ("the claims"), sustained or asserted against the State for personal injury, death, or property loss or damage, arising out of, resulting from, or attributable to the willful misconduct, negligence, error, or omission of the Contractor, its employees, Subcontractors, consultants, representatives, and agents, resulting from this contract, except to the extent such Contractor liability is attenuated by any action of the State which directly and proximately contributed to the claims.

2. **INTELLECTUAL PROPERTY**
The Contractor agrees it will, at its sole cost and expense, defend, indemnify, and hold harmless the indemnified parties from and against any and all claims, to the extent such claims arise out of, result from, or are attributable to, the actual or alleged infringement or misappropriation of any patent, copyright, trade secret, trademark, or confidential information of any third party by the Contractor or its employees, Subcontractors, consultants, representatives, and agents; provided, however, the State gives the Contractor prompt notice in writing of the claim. The Contractor may not settle any infringement claim that will affect the State's use of the Licensed Software without the State's prior written consent, which consent may be withheld for any reason.

If a judgment or settlement is obtained or reasonably anticipated against the State's use of any intellectual property for which the Contractor has indemnified the State, the Contractor shall, at the Contractor's sole cost and expense, promptly modify the item or items which were determined to be infringing, acquire a license or licenses on the State's behalf to provide the necessary rights to the State to eliminate the infringement, or provide the State with a non-infringing substitute that provides the State the same functionality. At the State's election, the actual or anticipated judgment may be treated as a breach of warranty by the Contractor, and the State may receive the remedies provided under this RFP.

3. **PERSONNEL**
The Contractor shall, at its expense, indemnify and hold harmless the indemnified parties from and against any claim with respect to withholding taxes, worker's compensation, employee benefits, or any other claim, demand, liability, damage, or loss of any nature relating to any of the personnel, including subcontractor's and their employees, provided by the Contractor.

4. **SELF-INSURANCE**
The State of Nebraska is self-insured for any loss and purchases excess insurance coverage pursuant to Neb. Rev. Stat. § 81-8,239.01 (Reissue 2008). If there is a presumed loss under the provisions of this agreement, Contractor may file a claim with the Office of Risk Management pursuant to Neb. Rev. Stat. §§ 81-8,829 - 81-8,306 for review by the State Claims Board. The State retains all rights and immunities under the State Miscellaneous (Section 81-8,294), Tort (Section 81-8,209), and Contract Claim Acts (Section 81-8,302), as outlined in Neb. Rev. Stat. § 81-8,209 et seq. and under any other provisions of law and accepts liability under this agreement to the extent provided by law.

5. The Parties acknowledge that Attorney General for the State of Nebraska is required by statute to represent the legal interests of the State, and that any provision of this indemnity clause is subject to the statutory authority of the Attorney General.

K. ATTORNEY'S FEES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

In the event of any litigation, appeal, or other legal action to enforce any provision of the contract, the Parties agree to pay all expenses of such action, as permitted by law and if order by the court, including

attorney's fees and costs, if the other Party prevails.

L. ASSIGNMENT, SALE, OR MERGER

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

Either Party may assign the contract upon mutual written agreement of the other Party. Such agreement shall not be unreasonably withheld.

The Contractor retains the right to enter into a sale, merger, acquisition, internal reorganization, or similar transaction involving Contractor's business. Contractor agrees to cooperate with the State in executing amendments to the contract to allow for the transaction. If a third party or entity is involved in the transaction, the Contractor will remain responsible for performance of the contract until such time as the person or entity involved in the transaction agrees in writing to be contractually bound by this contract and perform all obligations of the contract.

M. CONTRACTING WITH OTHER NEBRASKA POLITICAL SUB-DIVISIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The Contractor may, but shall not be required to, allow agencies, as defined in Neb. Rev. Stat. §81-145, to use this contract. The terms and conditions, including price, of the contract may not be amended. The State shall not be contractually obligated or liable for any contract entered into pursuant to this clause. A listing of Nebraska political subdivisions may be found at the website of the Nebraska Auditor of Public Accounts.

N. FORCE MAJEURE

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

Neither Party shall be liable for any costs or damages, or for default resulting from its inability to perform any of its obligations under the contract due to a natural or manmade event outside the control and not the fault of the affected Party ("Force Majeure Event"). The Party so affected shall immediately make a written request for relief to the other Party, and shall have the burden of proof to justify the request. The other Party may grant the relief requested; relief may not be unreasonably withheld. Labor disputes with the impacted Party's own employees will not be considered a Force Majeure Event.

O. CONFIDENTIALITY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

All materials and information provided by the Parties or acquired by a Party on behalf of the other Party shall be regarded as confidential information. All materials and information provided or acquired shall be handled in accordance with federal and state law, and ethical standards. Should said confidentiality be breached by a Party, the Party shall notify the other Party immediately of said breach and take immediate corrective action.

It is incumbent upon the Parties to inform their officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a (i)(1), which is made applicable by 5 U.S.C. 552a (m)(1), provides that any officer or employee, who by virtue of his/her employment or official position has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

P. **OFFICE OF PUBLIC COUNSEL (Statutory)**
If it provides, under the terms of this contract and on behalf of the State of Nebraska, health and human services to individuals; service delivery; service coordination; or case management, Contractor shall submit to the jurisdiction of the Office of Public Counsel, pursuant to Neb. Rev. Stat. §§ 81-8,240 et seq. This section shall survive the termination of this contract.

Q. **LONG-TERM CARE OMBUDSMAN (Statutory)**
Contractor must comply with the Long-Term Care Ombudsman Act, Neb. Rev. Stat. §§ 81-2237 et seq. This section shall survive the termination of this contract.

R. **EARLY TERMINATION**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The contract may be terminated as follows:

1. The State and the Contractor, by mutual written agreement, may terminate the contract at any time.
2. The State, in its sole discretion, may terminate the contract for any reason upon thirty (30) calendar day's written notice to the Contractor. Such termination shall not relieve the Contractor of warranty or other service obligations incurred under the terms of the contract. In the event of termination the Contractor shall be entitled to payment, determined on a pro rata basis, for products or services satisfactorily performed or provided.
3. The State may terminate the contract immediately for the following reasons:

    a. if directed to do so by statute;
    b. Contractor has made an assignment for the benefit of creditors, has admitted in writing its inability to pay debts as they mature, or has ceased operating in the normal course of business;

c. a trustee or receiver of the Contractor or of any substantial part of the Contractor's assets has been appointed by a court;
d. fraud, misappropriation, embezzlement, malfeasance, misfeasance, or illegal conduct pertaining to performance under the contract by its Contractor, its employees, officers, directors, or shareholders;
e. an involuntary proceeding has been commenced by any Party against the Contractor under any one of the chapters of Title 11 of the United States Code and (i) the proceeding has been pending for at least sixty (60) calendar days; or (ii) the Contractor has consented, either expressly or by operation of law, to the entry of an order for relief; or (iii) the Contractor has been decreed or adjudged a debtor;
f. a voluntary petition has been filed by the Contractor under any of the chapters of Title 11 of the United States Code;
g. Contractor intentionally discloses confidential information;
h. Contractor has or announces it will discontinue support of the deliverable; and,
i. In the event funding is no longer available.

S. CONTRACT CLOSEOUT

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

Upon contract closeout for any reason the Contractor shall within 30 days, unless stated otherwise herein:

1. Transfer all completed or partially completed deliverables to the State;
2. Transfer ownership and title to all completed or partially completed deliverables to the State;
3. Return to the State all information and data, unless the Contractor is permitted to keep the information or data by contract or rule of law. Contractor may retain one copy of any information or data as required to comply with applicable work product documentation standards or as are automatically retained in the course of Contractor's routine back up procedures;
4. Cooperate with any successor Contactor, person or entity in the assumption of any or all of the obligations of this contract;
5. Cooperate with any successor Contactor, person or entity with the transfer of information or data related to this contract;
6. Return or vacate any state owned real or personal property; and,
7. Return all data in a mutually acceptable format and manner.

Nothing in this Section should be construed to require the Contractor to surrender intellectual property, real or personal property, or information or data owned by the Contractor for which the State has no legal claim.

II. CONTRACTOR DUTIES

A. INDEPENDENT CONTRACTOR / OBLIGATIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

It is agreed that the Contractor is an independent contractor and that nothing contained herein is intended or should be construed as creating or establishing a relationship of employment, agency, or a partnership.

The Contractor is solely responsible for fulfilling the contract. The Contractor or the Contractor's representative shall be the sole point of contact regarding all contractual matters.

The Contractor shall secure, at its own expense, all personnel required to perform the services under the contract. The personnel the Contractor uses to fulfill the contract shall have no contractual or other legal relationship with the State; they shall not be considered employees of the State and shall not be entitled to any compensation, rights or benefits from the State, including but not limited to, tenure rights, medical and hospital care, sick and vacation leave, severance pay, or retirement benefits.

By-name personnel commitments made in the Contractor's proposal shall not be changed without the prior written approval of the State. Replacement of these personnel, if approved by the State, shall be with personnel of equal or greater ability and qualifications.

All personnel assigned by the Contractor to the contract shall be employees of the Contractor or a subcontractor, and shall be fully qualified to perform the work required herein. Personnel employed by the Contractor or a subcontractor to fulfill the terms of the contract shall remain under the sole direction and control of the Contractor or the subcontractor respectively.

With respect to its employees, the Contractor agrees to be solely responsible for the following:

1. Any and all pay, benefits, and employment taxes and/or other payroll withholding;
2. Any and all vehicles used by the Contractor's employees, including all insurance required by state law;
3. Damages incurred by Contractor's employees within the scope of their duties under the contract;
4. Maintaining Workers' Compensation and health insurance that complies with state and federal law and submitting any reports on such insurance to the extent required by governing law; and
5. Determining the hours to be worked and the duties to be performed by the Contractor's employees.
6. All claims on behalf of any person arising out of employment or alleged employment (including without limit claims of discrimination alleged against the Contractor, its officers, agents, or subcontractors or subcontractor's employees)

If the Contractor intends to utilize any subcontractor, the subcontractor's level of effort, tasks, and time allocation should be clearly defined in the bidder's proposal. The Contractor shall agree that it will not utilize any subcontractors not specifically included in its proposal in the performance of the contract without the prior written authorization of the State.

The State reserves the right to require the Contractor to reassign or remove from the project any Contractor or subcontractor employee.

Contractor shall insure that the terms and conditions contained in any contract with a subcontractor does not conflict with the terms and conditions of this contract.

The Contractor shall include a similar provision, for the protection of the State, in the contract with any

Subcontractor engaged to perform work on this contract.

B. **EMPLOYEE WORK ELIGIBILITY STATUS**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The Contractor is required and hereby agrees to use a federal immigration verification system to determine the work eligibility status of employees physically performing services within the State of Nebraska. A federal immigration verification system means the electronic verification of the work authorization program authorized by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, 8 U.S.C. 1324a, known as the E-Verify Program, or an equivalent federal program designated by the United States Department of Homeland Security or other federal agency authorized to verify the work eligibility status of an employee.

If the Contractor is an individual or sole proprietorship, the following applies:

1. The Contractor must complete the United States Citizenship Attestation Form, available on the Department of Administrative Services website at http://das.nebraska.gov/materiel/purchasing.html

   The completed United States Attestation Form should be submitted with the RFP response.

2. If the Contractor indicates on such attestation form that he or she is a qualified alien, the Contractor agrees to provide the US Citizenship and Immigration Services documentation required to verify the Contractor's lawful presence in the United States using the Systematic Alien Verification for Entitlements (SAVE) Program.

3. The Contractor understands and agrees that lawful presence in the United States is required and the Contractor may be disqualified or the contract terminated if such lawful presence cannot be verified as required by Neb. Rev. Stat. §4-108.

C. **COMPLIANCE WITH CIVIL RIGHTS LAWS AND EQUAL OPPORTUNITY EMPLOYMENT / NONDISCRIMINATION (Statutory)**

The Contractor shall comply with all applicable local, state, and federal statutes and regulations regarding civil rights laws and equal opportunity employment. The Nebraska Fair Employment Practice Act prohibits Contractors of the State of Nebraska, and their Subcontractors, from discriminating against any employee or applicant for employment, with respect to hire, tenure, terms, conditions, compensation, or privileges of employment because of race, color, religion, sex, disability, marital status, or national origin (Neb. Rev. Stat. §48-1101 to 48-1125). The Contractor guarantees compliance with the Nebraska Fair Employment Practice Act, and breach of this provision shall be regarded as a material breach of contract. The Contractor shall insert a similar provision in all Subcontracts for services to be covered by any contract resulting from this RFP.

D. COOPERATION WITH OTHER CONTRACTORS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

Contractor may be required to work with or in close proximity to other contractors or individuals that may be working on same or different projects. The Contractor shall agree to cooperate with such other contractors or individuals, and shall not commit or permit any act which may interfere with the performance of work by any other contractor or individual. Contractor is not required to compromise Contractor's intellectual property or proprietary information unless expressly required to do so by this contract.

E. PERMITS, REGULATIONS, LAWS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The contract price shall include the cost of all royalties, licenses, permits, and approvals, whether arising from patents, trademarks, copyrights or otherwise, that are in any way involved in the contract. The Contractor shall obtain and pay for all royalties, licenses, and permits, and approvals necessary for the execution of the contract. The Contractor must guarantee that it has the full legal right to the materials, supplies, equipment, software, and other items used to execute this contract.

F. OWNERSHIP OF INFORMATION AND DATA / DELIVERABLES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The State shall have the unlimited right to publish, duplicate, use, and disclose all information and data developed or obtained by the Contractor on behalf of the State pursuant to this contract.

The State shall own and hold exclusive title to any deliverable developed as a result of this contract. Contractor shall have no ownership interest or title, and shall not patent, license, or copyright, duplicate, transfer, sell, or exchange, the design, specifications, concept, or deliverable.

G. INSURANCE REQUIREMENTS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The Contractor shall throughout the term of the contract maintain insurance as specified herein and provide the State a current Certificate of Insurance/Acord Form (COI) verifying the coverage. The Contractor shall not commence work on the contract until the insurance is in place. If Contractor subcontracts any portion of the Contract the Contractor must, throughout the term of the contract, either:

1. Provide equivalent insurance for each subcontractor and provide a COI verifying the coverage for the subcontractor;
2. Require each subcontractor to have equivalent insurance and provide written notice to the State that the Contractor has verified that each subcontractor has the required coverage; or,
3. Provide the State with copies of each subcontractor's Certificate of Insurance evidencing the required coverage.

The Contractor shall not allow any Subcontractor to commence work until the Subcontractor has equivalent insurance. The failure of the State to require a COI, or the failure of the Contractor to provide a COI or require subcontractor insurance shall not limit, relieve, or decrease the liability of the Contractor hereunder.

In the event that any policy written on a claims-made basis terminates or is canceled during the term of the contract or within five (5) years of termination or expiration of the contract, the contractor shall obtain an extended discovery or reporting period, or a new insurance policy, providing coverage required by this contract for the term of the contract and five (5) years following termination or expiration of the contract.

If by the terms of any insurance a mandatory deductible is required, or if the Contractor elects to increase the mandatory deductible amount, the Contractor shall be responsible for payment of the amount of the deductible in the event of a paid claim.

Notwithstanding any other clause in this Contract, the State may recover up to the liability limits of the insurance policies required herein.

1. WORKERS' COMPENSATION INSURANCE
The Contractor shall take out and maintain during the life of this contract the statutory Workers' Compensation and Employer's Liability Insurance for all of the contactors' employees to be engaged in work on the project under this contract and, in case any such work is sublet, the Contractor shall require the Subcontractor similarly to provide Worker's Compensation and Employer's Liability Insurance for all of the Subcontractor's employees to be engaged in such work. This policy shall be written to meet the statutory requirements for the state in which the work is to be performed, including Occupational Disease. **The policy shall include a waiver of subrogation in favor of the State. The COI shall contain the mandatory COI subrogation waiver language found hereinafter**. The amounts of such insurance shall not be less than the limits stated hereinafter. For employees working in the State of Nebraska, the policy must be written by an entity authorized by the State of Nebraska Department of Insurance to write Workers' Compensation and Employer's Liability Insurance for Nebraska employees.

2. COMMERCIAL GENERAL LIABILITY INSURANCE AND COMMERCIAL AUTOMOBILE LIABILITY INSURANCE
The Contractor shall take out and maintain during the life of this contract such Commercial General Liability Insurance and Commercial Automobile Liability Insurance as shall protect

Contractor and any Subcontractor performing work covered by this contract from claims for damages for bodily injury, including death, as well as from claims for property damage, which may arise from operations under this contract, whether such operation be by the Contractor or by any Subcontractor or by anyone directly or indirectly employed by either of them, and the amounts of such insurance shall not be less than limits stated hereinafter.

The Commercial General Liability Insurance shall be written on an **occurrence basis**, and provide Premises/Operations, Products/Completed Operations, Independent Contractors, Personal Injury, and Contractual Liability coverage. **The policy shall include the State, and others as required by the contract documents, as Additional Insured(s). This policy shall be primary, and any insurance or self-insurance carried by the State shall be considered secondary and non-contributory. The COI shall contain the mandatory COI liability waiver language found hereinafter.** The Commercial Automobile Liability Insurance shall be written to cover all Owned, Non-owned, and Hired vehicles.

REQUIRED INSURANCE COVERAGE	
COMMERCIAL GENERAL LIABILITY	
General Aggregate	$2,000,000
Products/Completed Operations Aggregate	$2,000,000
Personal/Advertising Injury	$1,000,000 per occurrence
Bodily Injury/Property Damage	$1,000,000 per occurrence
Medical Payments	$10,000 any one person
Damage to Rented Premises (Fire)	$300,000 each occurrence
Contractual	Included
Independent Contractors	Included
If higher limits are required, the Umbrella/Excess Liability limits are allowed to satisfy the higher limit.	
WORKER'S COMPENSATION	
Employers Liability Limits	$500K/$500K/$500K
Statutory Limits- All States	Statutory - State of Nebraska
Voluntary Compensation	Statutory
COMMERCIAL AUTOMOBILE LIABILITY	
Bodily Injury/Property Damage	$1,000,000 combined single limit
Include All Owned, Hired & Non-Owned Automobile liability	Included
Motor Carrier Act Endorsement	Where Applicable
UMBRELLA/EXCESS LIABILITY	
Over Primary Insurance	$5,000,000 per occurrence
PROFESSIONAL LIABILITY	
All Other Professional Liability (Errors & Omissions)	$1,000,000 Per Claim / Aggregate
COMMERCIAL CRIME	
Crime/Employee Dishonesty Including 3rd Party Fidelity	$1,000,000
CYBER LIABILITY	
Breach of Privacy, Security Breach, Denial of Service, Remediation, Fines and Penalties	$10,000,000
MANDATORY COI SUBROGATION WAIVER LANGUAGE	
"Workers' Compensation policy shall include a waiver of subrogation in favor of the State of Nebraska."	
MANDATORY COI LIABILITY WAIVER LANGUAGE	
"Commercial General Liability & Commercial Automobile Liability policies shall name the State of Nebraska as an Additional Insured and the policies shall be primary and any insurance or self- insurance carried by the State shall be considered secondary and non-contributory as additionally insured."	

If the mandatory COI subrogation waiver language or mandatory COI liability waiver language on the COI states that the waiver is subject to, condition upon, or otherwise limit by the insurance policy, a copy of the relevant sections of the policy must be submitted with the COI so the State can review the limitations imposed by the insurance policy.

3. EVIDENCE OF COVERAGE

The Contractor shall furnish the Contract Manager, with a certificate of insurance coverage complying with the above requirements prior to beginning work at:

Department of Health and Human
Services State Unit on Aging
Medicaid and Long Term
Care Attn: Contract
Manager
PO Box 95026
Lincoln, NE 68509

These certificates or the cover sheet shall reference the RFP number, and the certificates shall include the name of the company, policy numbers, effective dates, dates of expiration, and amounts and types of

coverage afforded. If the State is damaged by the failure of the Contractor to maintain such insurance, then the Contractor shall be responsible for all reasonable costs properly attributable thereto.

Reasonable notice of cancellation of any required insurance policy must be submitted to the contract manager as listed above when issued and a new coverage binder shall be submitted immediately to ensure no break in coverage.

4. DEVIATIONS

The insurance requirements are subject to limited negotiation. Negotiation typically includes, but is not necessarily limited to, the correct type of coverage, necessity for Workers' Compensation, and the type of automobile coverage carried by the Contractor.

H. ANTITRUST

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The Contractor hereby assigns to the State any and all claims for overcharges as to goods and/or services provided in connection with this contract resulting from antitrust violations which arise under antitrust laws of the United States and the antitrust laws of the State.

I. CONFLICT OF INTEREST

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

By submitting a proposal, bidder certifies that there does not now exist a relationship between the bidder and any person or entity which is or gives the appearance of a conflict of interest related to this RFP or project.

The bidder certifies that it shall not take any action or acquire any interest, either directly or indirectly, which will conflict in any manner or degree with the performance of its services hereunder or which creates an actual or an appearance of conflict of interest.

The bidder certifies that it will not knowingly employ any individual known by bidder to have a conflict of interest.

The Parties shall not knowingly, for a period of two years after execution of the contract, recruit or employ any employee or agent of the other Party who has worked on the RFP or project, or who had any influence on decisions affecting the RFP or project.

J. STATE PROPERTY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The Contractor shall be responsible for the proper care and custody of any State-owned property which is furnished for the Contractor's use during the performance of the contract. The Contractor shall reimburse the State for any loss or damage of such property; normal wear and tear is expected.

K. SITE RULES AND REGULATIONS

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The Contractor shall use its best efforts to ensure that its employees, agents, and Subcontractors comply with site rules and regulations while on State premises. If the Contractor must perform on-site work outside of the daily operational hours set forth by the State, it must make arrangements with the State to ensure access to the facility and the equipment has been arranged. No additional payment will be made by the State on the basis of lack of access, unless the State fails to provide access as agreed to in writing between the State and the Contractor.

L. ADVERTISING

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The Contractor agrees not to refer to the contract award in advertising in such a manner as to state or imply that the company or its services are endorsed or preferred by the State. Any publicity releases pertaining to the project shall not be issued without prior written approval from the State.

M. NEBRASKA TECHNOLOGY ACCESS STANDARDS (Statutory)

Contractor shall review the Nebraska Technology Access Standards, found at http://nitc.nebraska.gov/standards/2- 201.html and ensure that products and/or services provided under the contract are in compliance or will comply with the applicable standards to the greatest degree possible. In the event such standards change during the Contractor's performance, the State may create an amendment to the contract to request the contract comply with the changed standard at a cost mutually acceptable to the parties.

N. BUSINESS CONTINUITY/DISASTER RECOVERY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The Contractor shall have a disaster recovery and back-up plan, of which a copy should be provided upon request to the State, which includes, but is not limited to equipment, personnel, facilities, and transportation, in order to continue services as specified under the specifications in the contract in the event of a disaster.

Additional requirements for the Business Continuity/Disaster Recovery Plan included in Section V.E.1.8.

O. DRUG POLICY

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

Contractor certifies it maintains a drug free work place environment to ensure worker safety and workplace integrity. Contractor agrees to provide a copy of its drug free workplace policy at any time upon request by the State.

IV. PAYMENT

A. PROHIBITION AGAINST ADVANCE PAYMENT (Statutory)
Payments shall not be made until contractual deliverable(s) are received and accepted by the State.

B. TAXES (Statutory)
The State is not required to pay taxes and assumes no such liability as a result of this solicitation. Any property tax payable on the Contractor's equipment which may be installed in a state-owned facility is the responsibility of the Contractor.

C. INVOICES

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

Invoices for payments must be submitted by the Contractor to the agency requesting the services with sufficient detail to support payment.

Administrator - State Unit on
Aging 301 Centennial Mall S.
Lincoln, NE 68508

The terms and conditions included in the Contractor's invoice shall be deemed to be solely for the convenience of the parties. No terms or conditions of any such invoice shall be binding upon the State, and no action by the State, including without limitation the payment of any such invoice in whole or in part, shall be construed as binding or estopping the State with respect to any such term or condition, unless the invoice term or condition has been previously agreed to by the State as an amendment to the contract.

D. INSPECTION AND APPROVAL

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

Final inspection and approval of all work required under the contract shall be performed by the designated State officials.

The State and/or its authorized representatives shall have the right to enter any premises where the Contractor or Subcontractor duties under the contract are being performed, and to inspect, monitor or otherwise evaluate the work being performed. All inspections and evaluations shall be at reasonable times and in a manner that will not unreasonably delay work.

E. **PAYMENT**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

State will render payment to Contractor when the terms and conditions of the contract and specifications have been satisfactorily completed on the part of the Contractor as solely determined by the State. (Neb. Rev. Stat. Section 73-506(1)) Payment will be made by the responsible agency in compliance with the State of Nebraska Prompt Payment Act (See Neb. Rev. Stat. §81-2401 through 81-2408). The State may require the Contractor to accept payment by electronic means such as ACH deposit. In no event shall the State be responsible or liable to pay for any services provided by the Contractor prior to the Effective Date of the contract, and the Contractor hereby waives any claim or cause of action for any such services.

F. **LATE PAYMENT (Statutory)**
The Contractor may charge the responsible agency interest for late payment in compliance with the State of Nebraska Prompt Payment Act (See Neb. Rev. Stat. §81-2401 through 81-2408).

G. **SUBJECT TO FUNDING / FUNDING OUT CLAUSE FOR LOSS OF APPROPRIATIONS**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The State's obligation to pay amounts due on the Contract for a fiscal years following the current fiscal year is contingent upon legislative appropriation of funds. Should said funds not be appropriated, the State may terminate the contract with respect to those payments for the fiscal year(s) for which such funds are not appropriated. The State will give the Contractor written notice thirty (30) calendar days prior to the effective date of termination. All obligations of the State to make payments after the termination date will cease. The Contractor shall be entitled to receive just and equitable compensation for any authorized work which has been satisfactorily completed as of the termination date. In no event shall the Contractor be paid for a loss of anticipated profit.

A. RIGHT TO AUDIT (First Paragraph is Statutory)

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within RFP Response (Initial)	NOTES/COMMENTS:
T.O.			

The State shall have the right to audit the Contractor's performance of this contract upon a 30 days' written notice. Contractor shall utilize generally accepted accounting principles, and shall maintain the accounting records, and other records and information relevant to the contract (Information) to enable the State to audit the contract. The State may audit and the Contractor shall maintain, the Information during the term of the contract and for a period of five (5) years after the completion of this contract or until all issues or litigation are resolved, whichever is later. The Contractor shall make the Information available to the State at Contractor's place of business or a location acceptable to both Parties during normal business hours. If this is not practical or the Contractor so elects, the Contractor may provide electronic or paper copies of the Information. The State reserves the right to examine, make copies of, and take notes on any Information relevant to this contract, regardless of the form or the Information, how it is stored, or who possesses the Information. Under no circumstance will the Contractor be required to create or maintain documents not kept in the ordinary course of contractor's business operations, nor will contractor be required to disclose any information, including but not limited to product cost data, which is confidential or proprietary to contractor.

The Parties shall pay their own costs of the audit unless the audit finds a previously undisclosed overpayment by the State. If a previously undisclosed overpayment exceeds one-half of one percent (.5%) of the total contract billings, or if fraud, material misrepresentations, or non-performance is discovered on the part of the Contractor, the Contractor shall reimburse the State for the total costs of the audit. Overpayments and audit costs owed to the State shall be paid within ninety days of written notice of the claim. The Contractor agrees to correct any material weaknesses or condition found as a result of the audit.

SUMMARY OF BIDDER'S CORPORATE EXPERIENCE

The bidder should provide a summary matrix listing the bidder's previous projects similar to this RFP in size, scope, and complexity. The State will use no more than three (3) narrative project descriptions submitted by the bidder during its evaluation of the proposal. The bidder should address the following:

i. Provide narrative descriptions to highlight the similarities between the bidder's experience and this RFP. These descriptions should include:

a) The time period of the project;

b) The scheduled and actual completion dates;

c) The Contractor's responsibilities;

d) For reference purposes, a customer name (including the name of a contact person, a current telephone number, a facsimile number, and e-mail address); and

e) Each project description should identify whether the work was performed as the prime Contractor or as a Subcontractor. If a bidder performed as the prime Contractor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.

ii. Contractor and Subcontractor(s) experience should be listed separately. Narrative descriptions submitted for Subcontractors should be specifically identified as Subcontractor projects.

iii. If the work was performed as a Subcontractor, the narrative description should identify the same information as requested for the Contractors above. In addition, Subcontractors should identify what share of contract costs, project responsibilities, and time period were performed as a Subcontractor.

Please see our Summary Matrix, next page.

Remainder of page intentionally left blank.

VISUALVAULT PROJECT SUMMARY MATRIX

Name	Narrative Summary - Highlight Similarities	Time period	Scheduled & actual completion dates	Contractor's Responsibilities	Sub-Contractor	Contact Name	Phone	email	Prime Y/N
Florida Department of Children and Families	The Department of Children and Families has responsibility for oversight of the Substance Abuse and Mental Health program for the state. The VisualVault platform helps the department work with Service Providers to improve the level of care as well as greater oversight of service delivery. Our team is responsible for the rapid implementation of new content required to support the Department.	Jan. 2017 - August 2017	Completed on schedule. 7 months	Project Management, Workflow Development, User interface, Implementation planning, Data migration	Business and system analysis, business process integration, data strategy and management, Forms development, Business rules, Report creation, Data migration	Chris Weber	850 717 4266	chris.weber@myflfamilies.com	Y
Arizona Department of Gaming	VisualVault developed and implemented a gambling addiction treatment solution for Arizona Department of Gaming. This solution gives control and oversite for the management of providers, treatment of patients, service invoicing, PO limit management and collects data to support legislative reporting. From the first phase of implementation, additional modules have been added at least yearly to facilitate Outpatient, Intensive Outpatient, Residential and Group Treatment. Additionally, providers can receive remuneration for training and supporting other providers through the system. Implementation of this system provided the following benefits: • Visibility and process transparency became the standard. • Reporting was simplified by readily available data. • Control of funds allocated to a patient was traceable enabling the focus to return to improving treatment outcomes. • Spending was controlled and managed so that the budget was conserved and used for program growth. • Reports and dashboards provide real time updates for staff and management to view KPI data at any moment and provides the ability to drill into the data by simply clicking on the graphic. • Data required by legislatures is readily available to track successes and failures. This implementation allowed the Arizona Department of Gaming, Office of Problem Gambling to be able to manage their program with a handful of people amidst attrition of the original staff. Over time this solution was normalized to use the same configuration and business rules as other gambling addiction treatment systems implemented by VisualVault. Only slight configuration differences in business rules, invoicing and types of service are different from other implemented solutions.	Jan. 2010 - July 2010	Completed on schedule. 6 months	Project Management, Workflow Development, User interface, Implementation planning, Data migration, Business and system analysis, Business process integration, data strategy and management, Forms development, Business rules, Report creation		Elise Malofsen	602 255 3852	emalofsen@problemgambling.az.gov	Y
Pierce County Human Services, Billing and Outcome Systems	Pierce County Human Services sought bidding for a company to create a billing and outcome solution to provide services for individuals with Developmental Disabilities. This solution needed to manage individuals' authorizations, timelines, billing, verification to ensure pay versus pay for the Employments and Day Services Subsidies from, and Early Intervention programs. This solution helping individuals from the State of Washington's Department of Disability and Early Intervention Case Management agency to promote the creation of the individuals living in Pierce County. The report also between the authorizations for services assigned to providers within the county. Providers only see individuals where an authorization exists that belonged to the provider. The authorization is used to automate the process of payment requests and service recording every month. Providers may also batch report service information into the system on approved devices they provided to their clients. If current Requests follow an approval workflow to Federal Managers and approved by the provider, county staff and county fiscal staff. Service information required in the Washington Department of Disability as proof of service is easily accessible from the system. Finally, the system assists county staff the ability to monitor the program more closely, report new funding is being utilized and identify how patients volunteers. The system provides the ability to: - Record service providers hours worked by providers to support the de-employment disabilities programs manager - Import and export data and further external systems. Provider submitted systems - Secure Provider Access - Web Portals - Automate monthly reports on billable hours worked by service providers for County's program and list of averages of services funded by Developmental Disabilities Administration (DDA), Department of Early Learning Early Support for Infants and Toddlers (ESIT) Program, and School Districts, and to report to Human Development Disability Administration (DDA) Aging and Disability Services Web Account, Adult Case Mgt Information System (ACM), DDA's Form CMS - Data format to be compliance must follow requirements of "Billing Information Sheet for CMS Homemaker - All Services" - Provide real time reports and dashboards on outcomes per Funder and County requirements	Jan. 2018 - August 2018	Completed on schedule. 7 months	Project Management, Workflow Development, User interface, Implementation planning, Data migration, Business and system analysis, business process integration, data strategy and management, Forms development, Business rules, Report creation	platform configuration, modeling forms, workflows, business rule logic, report design and development	Marnee Adams	253 798 4332	madams@co.pierce.wa.us	Y

PROCOM CONSULTING PROJECT SUMMARY MATRIX

Frontier Communications	Frontier Communications has grown from $3B to over $10B in revenue by acquiring companies and properties from other telecommunications companies. For each of these acquisitions, Frontier has engage ProCom to provide system integration and/or data migration services to assist in migrating the acquired customer base to the Frontier application systems and environment. ProCom supported the business process integration, information technology and data integration ensuring flawless migration of millions of customers. Frontier engaged ProCom for over 15 major integration projects over 18 years.	1999 - 2019	15 individual projects completed on schedule	Program management, business and system analysis, business process integration, data strategy and management, application development, release management, and data conversion		Steven Ward	585-748-5746	steve.ward@ftr.com	Y
Mississippi Department of Human Services / Mississippi Department of Child Protection Services	The Mississippi legislature mandated the separation of the Family And Children's Services from the Human Services agency and the creation of a standalone agency. The work had to be done in a tight timeframe to meet court-ordered and legislative timeframes. The new agency had to stand up a fully sufficient Finance, Human Resources, and Information Technology Division as well as the facilities, contracts, and business of operations plan.	May 2016 through February 2018	Project completed 3 months ahead of original schedule	ProCom program assisted the separation project and advised the agency on best practices in each functional area. ProCom provided technology support to the IT Department for all application and support activities to support the separation.		Vick Jones	601-359-4442	Vick.Jones@mdcps.ms.gov	Y
Florida Agency for Health Care Administration	As part of the North Highland team, ProCom resources provided technical expertise to support the planning and project management for the Florida Agency for Health Care Administration program management office. This work was part of the overall Medicaid Enterprise System in accordance with US Center for Medicare and Medicaid Services (CMS) Conditions and Standards, including Medicaid Information Technology Architecture (MITA 3.0).	2017 through 2022	Program currently on schedule	Sub-contractor to North Highland with responsibility for the technical aspects of PMO including technology strategy, technical architecture, and overall program coordination. Work also included development of the Invitation to Negotiate for the Enterprise Data Warehouse module of the Medicaid Enterprise System as well as an overall technology roadmap for the program.	Y	Rick Zolzak	850-588-9295	rick.zolzak@northhighland.com	N

SUMMARY OF BIDDER'S PROPOSED PERSONNEL / MANAGEMENT APPROACH

The bidder should present a detailed description of its proposed approach to the management of the project.

The bidder should identify the specific professionals who will work on the State's project if their company is awarded the contract resulting from this RFP. The names and titles of the team proposed for assignment to the State project should be identified in full with a description of the team leadership, interface and support functions, and reporting relationships. The primary work assigned to each person should also be identified.

The bidder should provide resumes for all personnel proposed by the bidder to work on the project. The State will consider the resumes as a key indicator of the bidder's understanding of the skill mixes required to carry out the requirements of the RFP in addition to assessing the experience of specific individuals.

Resumes should not be longer than three (3) pages. Resumes should include, at a minimum, academic background and degrees, professional certifications, understanding of the process, and at least three (3) references (name, address, and telephone number) who can attest to the competence and skill level of the individual. Any changes in proposed personnel shall only be implemented after written approval from the State.

HYBRID WATERFALL/AGILE METHODOLOGY

The VisualVault Team will deploy a Hybrid Waterfall/Agile method to deliver the AIS solution. Our team uses this hybrid approach because we need to gain a deeper understanding of the requirements needs via an extensive discovery session. The outcome of this phase is our specification document. The specification document is a detailed listing of all functionality included in the AIS solution. NE stakeholders review the specification document to ensure it represents all functionality. Once the teams agree, the document is completed and signed. The SOW is updated to align with the specification document. At this point, the process moves to the Agile phase.

Our proposed approach for managing this project and Project Management Methodologies are documented and proven to be effective via hundreds of successful implementations. Please see: Attachment K1 Project Management and Testing Methodologies at the end of this proposal. A summary is found below.

VisualVault's Project Management Methodology is based upon PMBOK standards and our proven track record for successful delivery.

PRE-PLANNING SESSION

This session will be held to organize the implementation plan into the customers cadences, establish the roles and responsibilities across the implementation team, and ensure both the customer and VisualVault role & expected responsibilities are met. The pre-planning session will also identify the features/functions that will need to have current state business processes and procedures reviewed during Discovery.

BUSINESS ANALYSIS/DISCOVERY

During this phase of the project, we meet with subject matter experts, project stakeholders and customer leadership to understand the needs of the organization, the business processes, roles of individuals involved in the process, security and reporting needs. We seek to identify issues and bottle-necks in the current process. We seek to suggest solutions to resolve current issues.

Detailed requirements gathering is a key part of the Business Analysis phase. Detailed system requirements are generated that outline how the system will be configured to meet the needs and scope of the project.

Key work products include:

- Requirements that elaborate on the scope of work including business process flows, UI mockups, data validation rules, automation, security, anticipated data migration needs and key performance indicators
- Implementation strategy
- Conceptual sprint roadmap
- Resource staffing plan

- Defined current state of the business processes and procedures that require changes for future state
- Definition of reports and dashboards required
- Data conversion requirements and data conversion conceptual sprint plan
- Integration downstream and upstream blueprints

SPRINTS AND SPRINTS PLANNING

Sprints are a pre-defined period in which a specific unit of testable work is completed. Each Sprint starts with Sprint planning which includes further elaboration of the feature definitions documented during Discovery.

Sprint planning is completed by the project manager and implementation team members. However, the implementation team members have final say in the scope of each Sprint.

Sprint planning focuses on delivering a testable set of requirements as defined in the requirement specifications document. This approach allows the customer to begin testing early and continue testing throughout the project duration.

Each Sprint includes:
- Elaboration of a feature defined in the requirement specifications document
- System Development and Configuration
- Unit and feature testing
- Integration
- Demonstration
- Sprint Level User Acceptance Testing (UAT) by the customer
- Training
- Support Data Migration/Management

PRODUCTION IMPLEMENTATION

Feature components "exiting" from development Sprints and defined as 'done' are released into a "sandbox" environment. The Sandbox environment is a production like environment that will accumulate all 'done' feature components (including 'done' integrations). The Sandbox environment is considered a 'model office' environment that will be used 'on-going' by the business users to confirm business process and procedure changes, planning for training and communications and be a 'ready' product for production deployment.

The Production system is setup with configurations from the Sandbox environment. Once Solution / System User Acceptance Test is completed and the system is approved for production deployment, the VisualVault implementation team conducts final production migration.

PROJET CLOSEOUT AND SUPPORT

Once Project Acceptance has taken place the we start a 30-45-day transition period from our Professional Services team to our Support team. This transition means that issues will be logged in our Support system but will be managed by the team that delivered the solution to the customer.

PROJECT DELIVERABLES EXAMPLE

Deliverable	Description
Project Planning	
Project Plan Creation	Project plan creation and project setup
Business Analysis	
Discovery	
Specifications Document	Documents all required forms, business process flows, reports, customer business logic and data validation, external system integration requirements
Build Test Plan	Test plan will be created upon completion of requirements specification and updated as necessary during each sprint planning session
Data Migration	
Data Dictionary	Build data dictionary
Analysis	Perform analysis and document data migration tasks
Test Migrations	Perform test data migrations
Production Migration	Final production data migration
Testing	
Sprint Level UAT	**UAT performed on conclusion of each Sprint**
System-Level UAT & defect resolution	System Testing upon completion of each Program Increment
Integration Testing	Integration environment testing upon each sprint completion
Training Materials	
Customer Training Manual	Create training manual documenting all business processes
Training	
Train the Trainer (Typically one sessions @ 2 Day Training sessions or more as needed)	On-site classroom training
Admin Training (one conduct)	On-site classroom training
Post implementation webinars (As needed)	Online
Support Training (As needed)	On-site classroom training

The VisualVault Team was assembled based on the talent and expertise that aligns with NE requirements. All team members bring senior level skills and have been involved with implementing VisualVault in similar projects. In addition, we have the services of Mark Ervin as our Subject Matter Expert (SME). Mark was the CIO of Florida's Agency for Persons with Disabilities (APD). Mark led the procurement of a new platform to drive similar improvements in staff performance and service outcomes. Mark brings the insight of an individual who has walked in your shoes and will aid our team during the discovery process to avoid the risk areas that he encountered.

The VisualVault team brings the right business and technical skills necessary to complete the tasks in our proposed work plan according to the proposed schedule. Our Executive Sponsors have overall responsibility for the success of this project. Martha and Steve work closely with our project manager to understand the expectations and deliver the solution according to your requirements. Martha and Steve are also present to provide an additional communication line for NE's team should the need arise.

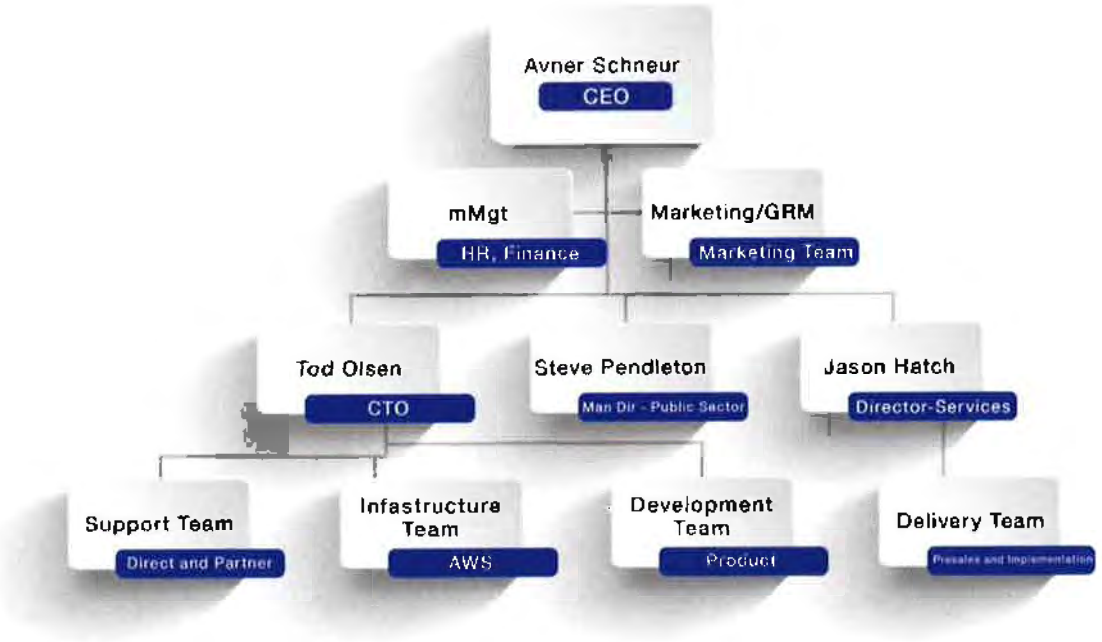
Our Quality Assurance lead works with our team to review deliverables and give an additional level of quality control to support the successful implementation of this project.

Our Project Manager leads the project planning activity and manages all resources, work assignments, schedules, risks, issues, and deliverables according to the agreed upon work plan.

Our Product Support Lead and Senior Software Engineers perform the implementation activities to configure the VisualVault platform. They lead the data migration work, the testing, and training work to provide continuity from requirements through go live.

Below please find an overview of the VisualVault team and a high-level view of our Staff.

VisualVault Organizational Chart



A subsidiary of GRM Information Management Services, Inc.

Remainder of page intentionally left blank.

Staff Overview

Steve Pendleton, Managing Director, Public Sector - Executive Sponsor

Steve Pendleton has an intimate understanding of government operations and the drive to continually improve service levels to an increasing number of constituents. Steve has 33 years of experience in Business Process Automation (BPA). As a BPA strategist, Steve developed the theory of the "Weight of Legacy" that described the root challenges inhibiting government's ability to modernize to achieve greatness. Successes as well as failures form restrictive institutional layers limiting an organization's ability to take actions to improve outcomes. The weight of the legacy success/failures and the high cost of outdated software licenses paralyze institutional change. Steve's work has proven state agencies can overcome the Weight of Legacy to achieve dramatic improvements and offers a track record of helping agencies deliver exceptional customer experiences while reducing staff stress and workloads. During his career, Steve has focused on automating data and document intensive business processes, virtually eliminating outdated paper-initiated activities (examples: licensing or compliance & enforcement activities) and compressing service times for core business processes by 30%-60%. The ability to migrate legacy hard copy documents processes to highly efficient digital processes enables agencies to do more with less and build elasticity into operations.

Martha Tuthill, Executive Vice President, ProCom Consulting LLC. - Executive Sponsor

Martha Tuthill has over 30 years of experience helping clients achieve better outcomes. Her experience includes public sector clients at the federal and state level as well as private industry experience. She has led large and small programs, run successful PMO organizations, served as the agency advocate overseeing large vendor contracts, and collaborated seamlessly across vendors to serve the end client. She has spent most of her career bridging the gap between the needs of the program and organizational leaders and the technology personnel who support them.

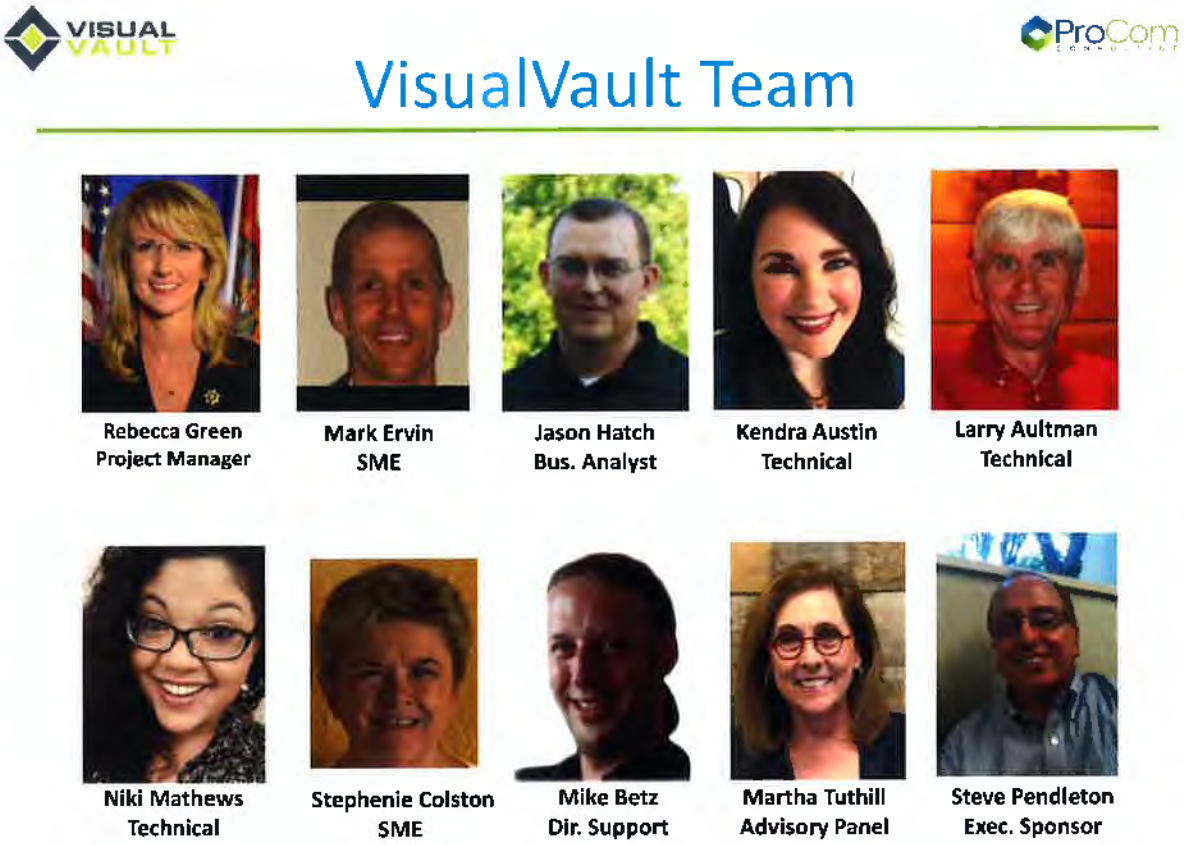
Mark Ervin, Former CIO of FL Department of Persons with Disabilities - SME

Mark Ervin is a focused technology and business professional with proven success in IT strategy/execution, managing diverse projects and complex enterprise IT operational environments across a variety of business and governmental segments. With Strong project and program management experience with SDLC projects including custom and commercial off-the-shelf (COTS) applications, technology infrastructure, and large managed services implementation, Mark will be intimately involved in this project, contributing his experiences to help us avoid potential problems and deliver successful outcomes.

Stephenie Colston, President Colston Consulting Group, LLC. - SME

Stephenie Colston is a dedicated senior professional with over 45 years of progressively responsible leadership and management experience in the private sector and in federal and state governments. She has a proven track record to identify, synthesize, and act upon complex policy and programmatic issues and to work effectively with senior executives including proprietary and private non-profit organizations, federal officials, state officials, stakeholders, foundations, trusts, associations, and boards of directors. She possesses expertise in a wide range of policy and program areas in substance abuse and mental health, demonstrating policy and political acumen. She has a strong track record of implementing performance - based cost saving measures, problem solving, and focusing on results. She spent 12 years as staff and Vice President of a national consulting firm, during which time she assessed dozens of State mental health and substance abuse agencies and hundreds of provider organizations using managerial, programmatic, data, and financial protocols and recommended operational process improvements to transform policies, processes, and technologies. She then became Senior Advisor for Substance Abuse for both the SAMHSA Administrator and the Director of the White House Office of National Drug Control Policy. After working as the SSA and SMHA for the State of Florida for several years, Ms. Colston created her own consulting company. Her consulting clients to date have included community-based substance abuse and mental health treatment and prevention organizations, homeless shelters, HIT companies, e- service organizations, private trusts/foundations, national associations, and state agencies. She has conducted hundreds of trainings relating to business process improvements, system of care improvements, and organizational change.

THE VISUALVAULT TEAM



Please see staff Resumes for primary personnel, next page.

PROPOSED STAFF RESUME

Company Name Submitting Proposal:	*ProCom Consulting Inc.*

Check the appropriate box if the proposed individual is prime contractor staff or subcontractor staff.			
Contractor:		Subcontractor:	*X*

The following information requested pertains to the individual being proposed for this project.			
Name:	*Martha Tuthill*	Key Personnel: (Yes/No)	*Yes*
Role:	*Executive Sponsor*		
# of Years in Relevant Project Experience:	*30*	# of Years with Firm:	*3*

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Martha has over 30 years of experience helping clients achieve better outcomes. Her experience includes public sector clients at the federal and state level as well as private industry experience. She has led large and small programs, run successful PMO organizations, served as the agency advocate overseeing large vendor contracts, and collaborated seamlessly across vendors to serve the end client. She has spent most of her career bridging the gap between the needs of the program and organizational leaders and the technology personnel who support them.

RELEVANT EXPERIENCE

North Carolina Program Evaluation Division
Executive Sponsor and Project Lead to support North Carolina Legislative Program Evaluation Division analysis of several large administrative programs including real estate holdings, facilities management, procurement of state term contracts, fleet management, incoming and outgoing mail costs, and parking management. Identified opportunities for efficiency improvements and cost savings.

Mississippi Department of Child Protection Services
Executive Sponsor and Project Lead to separate the Mississippi Department of Child Protection Services from the Mississippi Department of Human Services. Program managed the work to stand up the new agency's Finance, Human Resources, Information Technology, Facilities, Contracts, Property. and other administrative functions. Achieve the outcome four months ahead of legislatively mandated schedule.

South Carolina Commission for Higher Education
Advised the SC Commission for Higher Education on best practices in managing large data and providing more meaningful information to their stakeholders.

Texas Department of Families and Protective Services
Conducted an end-to-end assessment of Child Protective Services practices, policies, processes, and technologies. Identified high priority areas for transformation. Worked with agency to obtain funding for program and technology improvements. Worked with the 11 regions

across the state to implement each of the 20 high priority transformation projects to reduce costs, improve timeliness of service, and reduce attrition.

Florida Department of Children and Families

Worked with DCF to identify issues with the Florida Abuse Hotline and Child Protective Investigators. Worked with the Program and Regional personnel to identify people, processes, and technology issues and make recommendations to correct deficiencies. Worked with the Secretary to obtain legislative support to advance the Department's transformation agenda.

Advised the Florida Abuse Hotline on key components of an RFP for technology products and services. Assisted the Department on-board personnel to address technology challenges. Worked with personnel across multiple vendors to bring a web-based intake system live to reduce call volume and make it easier for professional reporters to communicate information to DCF.

Worked with the IT and Program leaders to understand requirements for the ITN for technology work to support the Child Welfare Transformation and the Statewide Automated Child Welfare Information System. Advised the Department on commercial best practices for project and enhancement work, service level agreements, and helped transition from the incumbent vendor to the new one to the agency.

Assisted the IT Department on high priority issues including their long-range Information Technology Strategic Plan, network security issues, email replacement, and implementation of Microsoft Office 365.

Arkansas Joint Legislative Task Force on Health Care Reform
Worked with the leaders of the Legislative Task Force to analyze Medicaid spend since the Affordable Care Act and recommend ways to reduce expenditures. Responsible for working with the Department of Human Services to analyze all technology expenditures and identify ways to reduce costs, improve service, and maintain health care coverage for the citizens of Arkansas.

Mississippi Department of Human Services
Assessed the Child Support Field Operations to assist the agency to make an insource/outsource decision. Coached the agency team on vendor procurement and RFP best practices. Advised the agency on a subsequent $30 million customer call center RFP.

Accenture
Served in a variety of leadership positions with Accenture including Chief Operating Office for the Communications and High-Tech Division as well as North American Delivery Lead for the Health and Public-Sector practice which include over 500 federal, state, and local government clients.

Project Executive responsible for the delivery of work to large federal agencies including U.S. Department of Education (PELL Grant program), Homeland Security (US VISIT), and the Internal Revenue Service (IRS.gov web site) to deliver complex, mission critical IT work.

Worked with large communications and energy companies. Part of a three-member leadership team that ran the 2000-person IT department for BellSouth for 6 years. Delivered customer care projects to improve customer service and reduce costs for over 10 electric and gas utilities.

EDUCATION

College of William and Mary, Bachelor of Arts in Economics and Computer Science

REFERENCES

Scott Stewart, Assistant Secretary for Administration, Florida Department of Children and Families, Scott.Stewart@myflfamilies.com, 850-717-4371

Colleen McCall, Director of Field Operations, Texas Department of Families and Protective Services (retired), ColleenWMcCall@gmail.com, 806-236-5303

PROPOSED STAFF RESUME

Company Name Submitting Proposal:	*ProCom Consulting Inc.*

Check the appropriate box if the proposed individual is prime contractor staff or subcontractor staff.			
Contractor:		**Subcontractor:**	*X*

The following information requested pertains to the individual being proposed for this project.			
Name:	*Rebecca Green*	**Key Personnel: (Yes/No)**	*Yes*
Classification; i.e., Project Manager, Implementation Lead, etc.	*Senior Implementation Project Manager*		
# of Years in Classification:	*13*	**# of Years with Firm:**	*1*

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE
Information should include a brief summary of the proposed individual's professional experience.

Rebecca has more than thirteen years of experience managing construction, business, and information technology solutions for public and private sector entities, including security, financial management, application development, disaster recovery, and business continuity and strategic program planning, as well as significant expertise in procurement and contract management within State of Florida government. Having formerly worked as part of the Florida Agency for State Technology (AST) team she possesses unique insight into the needs of State government and other customers. Rebecca has extensive experience developing competitive solicitations, including requirements gathering, for the State of Florida, has exceptional contract and legal expertise in the management of procurements which comply with State of Florida statute and rule, and more than three years of experience establishing and managing a State agency procurement office. She is a certified project management professional, an effective team leader, and excels at professional and complete communication among stakeholders, agency leadership, and technical staff.

RELEVANT EXPERIENCE
Information required should include: timeframe, company name, company location, position title held during the term of the project/position and software/hardware used during the project engagement.

ProCom Consulting, Inc. – October 2018 – present
Senior Project Manager managing enterprise and other VisualVault business process automation implementations in Florida and Vermont. Specific responsibilities include:

- Implementing large-scale VV business process automation software solutions.
- SDLS activities such as scoping, business analysis and requirements gathering, team management, quality assurance and user acceptance testing, risk assessment, and other efforts.
- Solicitation review and response, MS Project schedule and work breakdown structure development, TeamWork project management, etc.

SAS – November 2017 to October 2018
Senior Implementation Project Manager establishing an enterprise agency-wide data warehouse for the Florida Department of Transportation and Florida Water, as well as, Quantity/Quality data analytics and visualization projects for the University of Florida – Institute of Food and Agricultural Sciences, and the Florida Department of Environmental Protection. Specific responsibilities include:

- Implementing large-scale SAS visualization and analytics software.

- SDLS activities such as: scoping, requirements gathering, team management, quality assurance and user acceptance testing, risk assessment among others.

Imager Software Corporation – December 2016 to November 2017
Project and Account Manager managing large scale Information Technology projects focused around Microsoft Azure and Dynamics systems as well as Office 365 e-mail migrations. Clients included: Agency for Health Care Administration, the Department of Agriculture and Consumer Services, Executive Office of the Governor, Georgia Metropolitan Area Rapid Transit Authority, Florida State University Credit Union, City of North Miami Beach, and others. Specific responsibilities included:

- Statewide enterprise solicitation response development.
- Project technical documentation, fiscal oversight, and contract management

Florida Department of Corrections (FDC) – September 2015 to December 2016

Special Projects Manager July 2016 to December 2016
Responsible for solicitation development and process management; contract management; invoice processing management; and project management for multiple FY 2016/2017 high-visibility enterprise projects. Specific responsibilities included:

- Direct and indirect management of teams of 20 including managers, technical leads, subject matter experts, and software development staff.
- Coordinating with customers, stakeholders, and outsourced vendor staff.
- Supported CIO and executive strategic planning.

Bureau Chief and Business Solutions Support – September 2015 to July 2016
Identifying, developing, and directly managing project management, business analysis, and web development staff. Specific responsibilities included:

- Developed and maintained a bureau spend plan.
- Architected a new agency project management office and governance plan.
- Identified, evaluated, and managed agency project needs.
- Oversaw FDC Office 365 project which included reviewing all work products and processes to insure compliance with Florida Law, Administrative Code, and FDC policy.
- Managed the Kronos time keeping solution project's contract which included:
    - Invoicing, creation and facilitation of change orders and contract amendments, monitoring and management of performance metrics, development and maintenance of the project spend plan for legislative oversight, budget estimates, and other tasks.

Florida Agency for State Technology – December 2014 to September 2015
Project Manager and Procurement Administrator overseeing state agency information technology projects. Specific responsibilities included:

- Developed project management rules and guidelines for the State of Florida.
- PMO, process, and template development.
- Managed state enterprise IT Security Study Project, Data Feasibility Study project, Cloud Readiness Study project, and IT Security Testing project.
- Responsible for negotiation, procurement, and contract management of the enterprise disaster recovery implementation projects.

Florida Agency for State Technology Southwood Shared Resource Center – October 2011 to December 2014
Project Manager and Procurement Administrator leading multiple high-profile projects for the Agency, including the Enterprise I.T. Financial Management System and Security Event & Incident Management System. Specific responsibilities included:

- Managed the Enterprise Email statewide contract and procurement compliance with Florida Statutes.

- Developed and implemented a departmental procurement division, including the establishment of all necessary policies and procedures to ensure agency State of Florida procurement compliance.
- Developed complete agency documentation as needed, setting up of personnel roles, and other initiative tasks.
- Managed the development of various RFIs, RFPs, ITNs, and RFQs.
- Processed service level metric evaluations and billing for existing contracts.
- Extensive specification, business analysis, and scope development.
- Experience also included initial efforts as part of the statewide team working with the Florida Department of Financial Services to explore a statewide Travel System implementation.

Florida Department of Environmental Protection – March 2010 to October 2011

Contract Manager whose responsibilities included Office of Technology and Information Services procurement and solicitation development, issuance, evaluation, and management of I.T. contracts through to completion. Specific responsibilities included:

- Managed State Term Contract I.T. contractors in-house.
- Handled staff augmentation requests and management.
- Worked within MyFlorida MarketPlace (MFMP) including maintenance of PO and PR funds, creation of POs, and processing and payment of contractor invoicing with MFMP.
    - Created MFMP Direct (Purchase) Orders and Purchase Requisitions, Change Orders, E-Form invoicing, etc.
- Managed Daptiv Project Management contractor fund.
- Conducted business analysis, contract negotiation, contract and other technical writing, contract monitoring, and contract administration including close-out.

Florida Department of Health – August 2008 to March 2010

Office Automation Specialist administrating, maintaining, and updating computer application systems. Specific responsibilities included:

- Maintained, managed, and updated intranet web design.
- Administrative project management.
- SharePoint services and site maintenance.
- Team management duties including role as delegated supervisor, incident ticket assignment, and review and follow-up of outstanding work, workloads, and schedules.
- Web designer for pilot financial tracking system.

Ben Withers, Inc. – November 2005 to August 2008

Project and Contract Manager responsible for office, blueprint, and project management including: assessment, estimating, purchasing, shipping, construction, billing, collections, and reporting. Specific responsibilities included:

- Represented company with clients, subcontractors/vendors, and at-bid openings and other project meetings.
- Acted as Legal Secretary including creation and maintenance of contracts, liens, release of liens, etc.
- Extensive project research to support various claims.
- Filing of small claims issues for non-payment collections.
- Company representative at court proceedings.
- Responsible for all other company legal requirements.
- Acted as personal Secretary to the President: position included extensive letter-writing, file-management, calendar maintenance, customer service, travel arrangement, and presentation ability.
- Completed some training in Construction Estimating and Bid Techniques in April, 2007.
- Projects worked on included:
    - St. George Island State Park Campground and Bathhouse Renovations/Upgrade
    - Blackwater River State Park Campground and Bathhouse Renovations/Upgrade
    - Grayton Beach State Park – Park Improvements
    - Letchworth-Love Mounds Archaeological State Park – Day-Use Restroom

- Little Talbot Island Septic System Repair
- Paynes Prairie Preserve State Park – Alachua Sink Boardwalk
- City of St. Marks Boat Ramp

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

Florida State University, College of Interdisciplinary Social Sciences
Major/Minor: Public Administration/Political Science, Bachelor of Science, May 2017

Tallahassee Community College
Major: Business Administration, Associates of Arts, July 2014

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

- Project Management Professional (PMP) #1725601
- Certified Professional Public Buyer (CPPB) #12658
- ITIL 2007 (IT Infrastructure Library v.3)
- Florida Certified Public Manager (CPM)
- Florida Certified Contract Manager (FCCM) #467
- Florida Certified Supervisory Manager (CSM)
- Criminal Justice Information Services (CJIS) Compliant:
  - 2017 FL HSMV Level 2 Background Check Approved
  - 2016 FL FDLE Background Check approved
  - CJIS Security and Awareness Certified 2016

HARDWARE/SOFTWARE SUMMARY (BE SPECIFIC)

Information required should include: environments, hardware, software, tools and databases.

Project Management:

- Microsoft Project 2007 - 2016
- SharePoint Online

Office Automation:

- Windows 7, 8 & 10
- Microsoft Outlook, Excel, Word, Visio, and PowerPoint 2016

REFERENCES

A minimum of three (3) references are required, including name, phone number, fax number and email address.

Danielle Alvarez, Cybersecurity Strategist, danielle1.alvarez@gmail.com, 850-228-6753
Lincoln Quinton, President, North Point Consulting, Lincoln.quinton@thenorthpointe.com, 850-591-4377
Lance Kerwin, Profession, Florida State University, lkerwin@business.fsu.edu, 850-322-3001

PROPOSED STAFF RESUME

Company Name Submitting Proposal:	*VisualVault*

Check the appropriate box if the proposed individual is prime contractor staff or subcontractor staff.			
Contractor:	*X*	Subcontractor:	

The following information requested pertains to the individual being proposed for this project.			
Name:	*Jason Hatch*	Key Personnel: (Yes/No)	*Yes*
Classification; i.e., Project Manager, Implementation Lead, etc.	*Solution Architect*		
# of Years in Classification:	*8*	# of Years with Firm:	*13*

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

Seasoned IT leader with 22 years building technology solutions for startup and global organizations. Experienced in marketing, manufacturing, business and business technology consulting. Aptitude to manage multiple teams with situational leadership skills to drive projects and the success of the organization forward. Repeatable track record of trust and success with customers and partners. Ability to quickly adjust, learn and direct initiatives based on facts and goals.

Profession experiences include setting up and managing data centers and networks, acquiring software solutions to solve business problems and business consulting. Architected, managed the implementation and built solutions for California Department of Public Health, Arizona Department of Gaming, Florida Department of Children and Families and Pierce County Human Services.

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the project/position and software/hardware used during the project engagement.

Pierce County Washington, Human Services
Role: Solution Architect/Project Manager
Solution: Billing and Outcome System
Timeframe: January 2018 to Present

Summary: Sold, architected and let the project team in implementing this billing and outcome system. Project team included internal developers and external development staff. Solution includes automated import of client and authorization information from Washington State Department of Disability systems. Import marries individuals to providers and funding sources. System streamlines the process of providers entering service hours and job outcomes and then facilitates the approval of payment requests. Outcomes from the system are uploaded back to Washington State systems.

Florida Department of Children and Families, Office of Substance Abuse and Mental Health
Role: Solution Architect/Project Manager
Solution: Substance Abuse and Mental Health Provider Licensing System
Timeframe: January 2017 to August 2017

Summary: Served as the solution architect for this project. Conducted discovery sessions to produce the 200 page specifications document that ensured the solution met all statues, rules and business processes required. Managed the implementation team and assisted in the configuration, testing and

migration of legacy data. Developed and led the training sessions for the customer and their end users. Oversaw the development of product training manuals. The outcome was the solution was delivered on time and on budget. Supported customers through go live and into post production with complete satisfaction.

California Department of Public Health, Office of Problem Gambling
Role: Solution Architect/Project Manager
Solution: Gambling Addiction Treatment System
Timeframe: 2011 to Present

Summary: Architected and implemented the treatment system. Lead a non-technical customer through best practices and helped shape their business rules and program. When the system was implemented, user acceptance and rollout occurred in 3 months. The System interfaces were designed to enable providers who were computer novices providers could utilize with minimal training. Architected and added new services to the solution so the organization could provide Group, Intensive Outpatient and Residential Treatment. Continue to support the organization with yearly enhancements and updates to their system.

Arizona Department of Gaming, Office of Problem Gambling
Role: Solution Architect/Project Manager
Solution: Gambling Addiction Treatment System
Timeframe: 2010 to Present

Summary: Supported the original implementation of the system. In 2015, architected and helped migrate the original system to CA's common business rule based platform. Enhanced the business rules to use configurable variables that would enforce special processes used only by Arizona. Continue to support the organization to enhance their processes.

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

MASTERS OF BUSINESS ADMINISTRATION with focus on Management and Strategy
Western Governors University - April 2012

BACHELOR OF SCIENCE IN COMPUTER INFORMATION SYSTEMS
DeVry Institute of Technology - October 1998 - G.P.A. 3.72 Magna Cum Laude

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

Insert here any certifications proposed individual has received.

HARDWARE/SOFTWARE SUMMARY (BE SPECIFIC)

Information required should include: environments, hardware, software, tools and databases.

Use TSQL, JavaScript, HTML and other similar technologies to support and build business systems on BPM platform.

HTML/DHTML	IIS 6.0 and 7.5	DNS
JavaScript	SQL Server 2005 - 2012	PDMWorks
Sitefinity	VMWare 5.0	Epicor
VisualVault	TCP/IP	
Windows NT - 2012	Active Directory Admin	

REFERENCES

Cyndi Maivia, California Department of Public Health, Office of Problem Gambling
(916) 324-3948
cyndi.maivia@cdph.ca.gov

Elise Mikkelsen, Arizona Department of Gaming, Office of Problem Gambling
(602) 255-3852
emikkelsen@problemgambling.az.gov

Darren Jackson, Caliber Software
(623) 694-4926
darren.jackson@calibersoftware.com

PROPOSED STAFF RESUME

Company Name Submitting Proposal:	*ProCom Consulting Inc.*

Check the appropriate box if the proposed individual is prime contractor staff or subcontractor staff.			
Contractor:		Subcontractor:	*X*

The following information requested pertains to the individual being proposed for this project.			
Name:	*James Lawrence (Larry) Aultman*	Key Personnel: (Yes/No)	*Yes*
Classification; i.e., Project Manager, Implementation Lead, etc.	*Senior Developer*		
# of Years in Classification:	*35*	# of Years with Firm:	*1*

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

Larry is a Senior Developer specializing in web languages HTML 5, CSS3, and JavaScript including the modern TypeScript models. Experience includes working with line-of-business applications, critical business applications on the cloud or in the local data center. Larry has more than 30 years of experience as a Senior Developer and is well versed in multiple development languages platforms and works at all levels in applications development, configuration, and data integration.

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the project/position and software/hardware used during the project engagement.

Florida Dept. Children and Family (2018)
Senior Developer and Architect
Updating and proofing changes to Visual Vault documents due to legislative changes.

- Work with team to identify, correct, and update Visual Vault documents/forms used by the agency to validate compliance to statutes. Added additional functionallity to streamline workflows.

Pierce County, Washington (2018)
Senior Developer and Architect
Visual Vault updates and testing for final release of county data intake forms.

- Verify and test changes made to Visual Vault forms used by the county.

Dade County Health Department (2017-2018)
Senior Developer and Architect
Public Health Screening, Point of Dispense for Public Health, Health System Administration Services.

- Plan a totally new system built around three separate application profiles (public, internal use, and administration/reporting). The system must serve 1.2 million citizens in a 48 hour period. System allows self-screening, medications dispensing and administration/reporting.
  Development: HTML5/CSS3, JavaScript, TypeScript, Node.js, ASP.NET MVC/WebAPI/REST, .NET Core, C#, Transact SQL. Visual Studio, Visual Studio Code, other editors. **OSs**: SQL Server, Azure.
  Securtiy: Active Directory, Azure Active Directory, social media sign-on services.

Florida Department of Revenue (2015-2016)
Senior Developer and Architect

- Plan the migration of legacy systems to new redeveloped Platform as a Service (PaaS) cloud applications. The planned targets were Revenue Sharing (>$10 billion) redistribution to county government, Image Management System (>$3 billion) is an automated paper intake processing system.

Development: HTML5/CSS3/JQuery/BootStrap, JavaScript, TypeScript, Node.js, ASP.NET MVC/WebAPI/REST, .NET Core, C#, Transact SQL. Visual Studio, Visual Studio Code, other editors. **OSs**: Windows Server, SQL Server, Oracle, Azure.
Security: Active Directory, Azure Active Directory, social media sign-on services.

Florida Department of Health (2014-2015)

Senior Developer and Architect

- Developed a replacement Medical Quality Assurance Search Portal as a hybrid Azure cloud application hosted in the state datacenter as a cloud ready application.
- Developed a team and built a healthcare search portal for public use, replacing six data lookup sites with a modern user interface.
- Developed the Medical Quality Assurance IT architecture and the Agile Project Guidelines.
  Development: HTML5/CSS3/JQuery/BootStrap, JavaScript, TypeScript, Node.js, ASP.NET MVC/WebAPI/REST, .NET Core, C#, Transact SQL. Visual Studio, Visual Studio Code, other editors. **OSs**: Windows Server, SQL Server, Oracle, Azure.
  Security: Active Directory, Azure Active Directory, social media sign-on services.

Florida Department of Revenue (2013 - 2015)

Senior Developer

- Developed Agile team and architecture for a replacement application for paper form imaging system. The system processes approximately $3 billion in tax payer submissions.
- Developed the Standard Operating Environment architecture and the Agile Project Guidelines.
- Worked directly with CIO to develop the department's .NET strategy for future development including transiting applications to Azure cloud to develop PaaS applications.
  Development: HTML5/CSS3/JQuery/BootStrap, JavaScript, ASP.NET MVC/WebAPI/REST, .NET Core, C#, Transact SQL. Visual Studio, other editors. **OSs**: Windows Server, SQL Server, Oracle, Azure.
  Security: Active Directory, Azure Active Directory.

Microsoft - Blackbaud and Aderant (2013)

Senior Developer and Architect

- Architect for data migration and system design.
- Analyzed the business cases and created new architecture for future system development.
- Azure Strategist; developed strategy to move existing applications to Azure PaaS so that Aderant may offer SaaS to its clients.
  Development: HTML4/CSS, JavaScript, ASP.NET MVC/WebAPI/REST/WCF, .NET, C#, Transact SQL. Visual Studio, other editors. **OSs**: Windows Server, SQL Server, Oracle, Azure.
  Security: Active Directory, Azure Active Directory.

Florida House of Representatives, Redistricting Committee (2010-2011)

Senior Developer

- Developed a Microsoft Azure Cloud system to facilitate the 2010 US Census data incorporation into voting mapping districts for the State of Florida.
  Development: HTML4/CSS/Silverlight, JavaScript, ASP.NET MVC/WebAPI/WCF, .NET, C#, Transact SQL. Visual Studio, other editors. **OSs**: Windows Server, SQL Server, Oracle, Azure.
  Security: Active Directory.

Fringe Benefits Management Company (2009-2010)

Senior Developer

- Developed internal systems with the CIO and Director of IT to process employee benefits for healthcare purchases using VISA card services, processing claims for services in 24 states.
  Development: HTML4/CSS, JavaScript, ASP.NET MVC/WebAPI/WCF, .NET, C#, Transact SQL. Visual Studio, other editors. **OSs**: Windows Server, SQL Server, Oracle.
  Security: Active Directory.

Florida Agency for Workforce Innovation (2009-2010)

Senior Developer

- Assisted the CIO in developing a cloud computing strategy and discovery document.

Medical Messenger (2008-2009)

Senior Developer and Architect

- Software Architect advising on development of electronic medical records (EMR/EHR) system. **Development**: HTML4/CSS, JavaScript, ASP.NET MVC/WebAPI/REST, .NET, C#, Transact SQL. Visual Studio, other editors. **OSs**: Windows Server, SQL Server, Oracle, Azure. **Security**: Active Directory.

MedAffinity (2004-2008)

Senior Developer

- Developed a business for a start-up company as their system architect and designer. Worked with doctors and other healthcare provider to understand the financial and data reporting required by the Presidential Executive Order requiring all medical records to be in electronic form. **Development**: HTML4/CSS, JavaScript, ASP.NET MVC/WebAPI/REST, .NET, C#, Transact SQL. Visual Studio, other editors. **OSs**: Windows Server, SQL Server, Oracle, Azure.

Intact internal software development (2001-2007)

Senior Developer

- Redeveloped all internal systems converting all customer services to cloud based computing. Developed banking transaction processing through the Federal Reserve. Established banking relationships for online payment processing with Wachovia (Wells Fargo) for outbound funds transfers and with Modern Payment systems (BankServ) for inbound funds transfers.

Florida Department of State - June 2011 to April 2013

Chief Information Officer and Software Architect managing 35 developers and staff, managing IT services for six divisions. Specific responsibilities included:

- Developed and operated mission critical systems for 12 million voters in 67 county governments.
- Responsible for the architecture of new cloud computing systems in the multi-year modernization of legacy computing systems. Created process controls.
- Developed and operated mission critical systems for Division of Corporations including $350 million in revenue servicing 1.6 million corporations.
- Ensured a successful presidential election in Florida for the 2012 election cycle (presidential preference primary, primary, and general elections.)
- Evaluated statutory concerns in regard to application operation and deployment. Success is evidenced by a successful election cycle in Florida. There were no technical issues and no law suits were filed in connection with systems following the 2012 election.
- Developed system engineering, software engineering, system integration, and distributed system architectures.
- Established functional or system standards to ensure operational requirements, quality requirements, and design constraints are addressed.
- Documented design specifications, installation instructions, and other system-related information.
- Verified stability, interoperability, portability, security, or scalability of system architecture.
- Collaborated with software developers to select appropriate design solutions and ensure the compatibility of system components.
- Defined and analyzed objectives, scope, issues, or organizational impact of systems.
- Developed computer information resources, providing for data security and control, strategic computing, and disaster recovery. **Development**: HTML5/CSS3/JQuery, JavaScript, ASP.NET MVC/WebAPI/REST, .NET, C#, Transact SQL. Visual Studio, other editors. **OSs**: Windows Server, SQL Server, Oracle, Azure. **Security**: Active Directory.

Information Systems of Florida, Inc. - January 2008 to September 2008

Senior Developer and Consultant

- Consulted with users, management, vendors, and technicians to assess computing needs and system requirements.
- Evaluated data processing proposals to assess project feasibility and requirements.

SyncPac Corporation - February 1981 to May 2001

Company Founder and Chief Engineer focusing on industrial automation projects. Engineered global data center and internet development projects for large industrial concerns including E. I. DuPont, P&G, Scott Paper, Georgia Pacific, and Merck Chemical.

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

Samford University, Birmingham, AL, Bachelor's degree, August 1976

Abraham Baldwin Agricultural College, Tifton, GA, Associate of Science degree, June 1974

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

HARDWARE/SOFTWARE SUMMARY (BE SPECIFIC)

Information required should include: environments, hardware, software, tools and databases.

Development: HTML5/CSS3, JavaScript, TypeScript, Node.js, ASP.NET MVC/WebAPI/REST, .NET Core, C#, Transact SQL. Visual Studio, Visual Studio Code, other editors.
Operating Systems: SQL Server, Azure.
Securtiy: Active Directory, Azure Active Directory, social media sign-on services.

REFERENCES

Florida Department of Revenue:
Damu Kuttikrishnam, CIO, duttikrd@dor.state.fl.us, 850-717-7593

Florida Department of Health:
Joe Wright, Deputy CIO, joe.wright@flhealth.gov, 850-294-5801

Franklin County Planning and Zoning:
Michael Marone, Manager, michael@franklincountyflorida.com, 850-653-9783 ext. 155

SUBCONTRACTORS

If the bidder intends to Subcontract any part of its performance hereunder, the bidder shall provide:

i. name, address, and telephone number of the Subcontractor(s);
ii. specific tasks for each Subcontractor(s);
iii. percentage of performance hours intended for each Subcontract; and
iv. total percentage of Subcontractor(s) performance hours.

VisualVault's national Implementation partner is ProCom Consulting.

ProCom Consulting Inc.
15800 Birmingham Highway, Suite 400
Alpharetta, GA 30004
678-393-8610

For all tasks shown in the table below, the responsible party completes approximately 80% of the work hours and the supporting party completes approximately 20% of the work activities. Total hours per task is highlighted in our Implementation Plan included in our response.

Phase	Work Activity	Responsible Team	Support Team
Project Management	Project Planning	ProCom	
	Project Management	**ProCom**	
Business Analysis	Requirements Gathering	VisualVault	ProCom
	Form Specification	**ProCom**	**VisualVault**
	Report Specification	ProCom	VisualVault
	User Interface	**ProCom**	**VisualVault**
Implementation	Configuration	ProCom	VisualVault
	Automation	**ProCom**	**VisualVault**
Testing	Component / System Testing	ProCom	VisualVault
	User Acceptance Testing	**ProCom**	**VisualVault**
Training	Training Manual	VisualVault	ProCom
	End-User Training/Admin Training	**VisualVault**	**ProCom**
	Developer Training	VisualVault	ProCom
Data Migration	**Data Migration Planning**	**ProCom**	**VisualVault**
	Data Migration Implementation	ProCom	VisualVault

What Does This Mean for The Nebraska DHHS AIS System & Program?

1. ***Understands Requirements:*** *VisualVault has a solid understanding of the project, goals, and outcomes*
2. ***Top Team Talent:*** *The VisualVault Team assigned to the AIS project are all experienced senior team members with expertise delivering AIS and data migration*
3. ***Minimized Risk:*** *VisualVault uses a well-developed implementation approach used for dozens of highly successful projects*
4. ***Great Working Experience:*** *Looking back, DHHS team will say that we a great group of people to work with. We would do it again with the VisualVault Team.*

PAGES 56-74 HAV BEEN REDACTED DUE TO PROPRIETARY INFORMATION.

WWW.MAZARSUSA.COM

ACCOUNTING | TAX | CONSULTING

ATTACHMENT 2

Exhibit A – Hosting Agreement
Exhibit B – Acceptable Use Policy
Exhibit C – Support SLAs

Below please find:
Exhibit A - Hosting Agreement
Exhibit B - Acceptable Use Policy
Exhibit C - Support SLAs

Exhibit A Hosting Agreement

THIS AGREEMENT is made this ___ day of ____, 2018 by and between VisualVault, Inc., an Arizona corporation having its principal place of business at 2050 East ASU Circle, Suite 103, Tempe, Arizona 85284 ("VV") and Constellation Health LLC having its principal place of business at P.O. Box 360493, San Juan, PR 00936 ("Subscriber");

WHEREAS, VV is engaged in the cloud based enterprise content management software solutions services, including the capture, transfer, retention, workflow creation, and other business process improvement and other ancillary services in connection therewith, which allows Subscriber to access and retrieve Subscriber's stored content and data (collectively, the "Data") via the Internet (such services hereinafter collectively referred to as the "Services", and VV's software therefor, the "VV Software");

and

WHEREAS, the Subscriber has a need for such Services and the VV Software.

NOW, THEREFORE, in consideration of the mutual premises and covenants hereinafter set forth, the parties agree as follows;

1. **Term of Agreement** - The term of this Agreement shall commence on the _____, 2018 (the "Effective Date"), and will continue for sixty (60) months (the "Initial Term"), and shall be automatically renewed for successive one-year terms (each, a "Renewal Term" and together with the Initial Term, the "Term") unless written notice of non-renewal is delivered by either party to the other not less than sixty (60) days prior to the expiration of a Term

2. **Services**:
(a) VV will, internally or through a third-party servicer, cause the Services to be provided to Subscriber in accordance with the terms of this Agreement and any addendum attached thereto in the form of an exhibit (each an "Exhibit" and collectively, the "Exhibits"), including any Statement of Work (defined below). All Services shall be performed in accordance with the specifications and the time frames set forth in the Statement of Work, as may be modified from time to time in accordance with the terms of this Agreement. All Services shall be performed in accordance with VV's security, privacy, audit and compliance policies and standards. "Statement of Work" shall mean an addendum to this Agreement that defines a particular project for Subscriber to be undertaken by VV at the request of Subscriber, and shall include: (i) a description of the Services to be performed; (ii) the schedule on which such Services are to be developed and delivered, and (iii) the fees for the Services, which, unless otherwise provided, shall include a one-time charge for installation and account set-up. Upon execution, each such Statement of Work shall be deemed a part of this Agreement. To the extent that any provision contained in the Statement of Work is inconsistent with a provision set forth in this Agreement, such provision shall control. The first Statement of Work is attached hereto as Exhibit A.

(c)
3. **Payment for Services** - VV shall issue invoices on a monthly basis and payment shall be due within thirty (30) days of the invoice date. Charges for Services (including, but not limited to, storage charges and access charges) shall be in accordance with VV's standard pricing. VV shall be entitled to amend its prices and terms by providing prior written notice to Subscriber,

such notice to be delivered not less than ninety (90) days from the expiration date of the Term. Any payment not received by the due date shall be assessed a late fee of up to 10% of the outstanding unpaid sum and bear interest at 1.5 percent (1.50%) per month or the highest legal rate then in effect, if lower, from the due date until fully paid. If Subscriber fails to pay, VV may, upon written notice, declare the Subscriber in breach and suspend the provision of some or all of the Services to Subscriber. Subscriber shall pay all taxes, which may be levied or assessed in connection with this Agreement.

4. **Access to Data**
(a) The Subscriber will provide VV and/or its employees and agent's access to the Data being converted, wherever situated, to enable VV to perform the Services.
(b)VV shall use commercially reasonable efforts to make the Services available for use 24 hours a day, seven days per week (with the exception for scheduled maintenance downtown). The foregoing times of operation may be modified to provide for (a) regularly scheduled maintenance, (b) maintenance required as a result of matters beyond VV's reasonable control, or (c) events beyond VV's reasonable control. VV shall endeavor to give Subscriber at least twenty-four (24) hours' notice of scheduled maintenance will be provided by email to Subscriber's designated point of contact.

5. **Use Policy**
(a) All uses of the VV Software and the Services must comply with VV's use policy (hereinafter referred to as the "Use Policy") attached hereto as Exhibit B, which Use Policy may be amended from time-to-time. VV shall endeavor to give Subscriber notice of any such changes instituted in the Use Policy. VV reserves the right to suspend the Services or terminate this Agreement effective immediately upon notice to Subscriber's violation of the Use Policy.

(b) Subscriber (including Subscriber's authorized users) shall not engage or permit any unacceptable use of the Services. "Unacceptable use" of the Services shall include, but not be limited to, (a) dissemination or transmission (or establishment of links with the VV Software therefor) of material that, to a reasonable person, may be abusive, obscene, pornographic, defamatory, harassing, grossly offensive, vulgar, threatening or malicious; (b) dissemination or transmission of files, graphics, software or other material that actually or potentially infringes upon the copyright, trademark, patent, trade secret, or other intellectual property right of any person; (c) interference, disruption or attempt to gain unauthorized access to other accounts of VV or any other computer network; (d) dissemination or transmission of viruses, Trojan horses or any other malicious code or programs; or (e) engaging in any other activity reasonably considered by VV to conflict with the spirit and intent of this Agreement and/or the Services being rendered.

6. **Authorization** - Subscriber represents and warrants that it has the legal right and authority to enter into this Agreement and perform its obligations hereunder, and the performance of its obligations and the Services will not cause a breach of any agreements between Subscriber and any third parties.

7. **No Consequential Damages** - IN NO EVENT SHALL EITHER PARTY, ITS DIRECTORS, OFFICERS, EMPLOYEES, AGENTS OR AFFILIATES, BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES (EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBLITY OF SUCH DAMAGES) ARISING OUT OF THE PERFORMANCE, ATTEMPTED PERFORMANCE OR NON-PERFORMANCE OF THE SERVICES (OR PORTION THEREOF) HEREUNDER, INCLUDING, BUT NOT LIMITED TO, DAMAGES RESULTING FROM THE USE OF, OR INABIITY TO USE, THE SERVICES OR ANY PORTION THEREOF, DELAY OF DELIVERY OR COMPLETION OF THE SERVICES, INACCUARACY OR MISREPRESENTATION OF DATA, OR LOSS OF PROFITS, DATA, BUSINESS OR GOODWILL

8. **No Warranties** - EXCEPT AS EXPRESSLY SET FORTH HEREIN, VV MAKES NO EXPRESS WARRANTIES AND EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, TITLE AND FITNESS FOR A PARTICULAR PURPOSE. VV MAKES NO WARRANTY AS TO THE SUFFICIENCY OR SUITABILITY FOR SUBSCRIBER'S USE OF THE SERVICES FOR ANY PURPOSE, OR SPECIFIC REQUIREMENTS IN CONNECTION THEREWITH, OR THAT ACESS TO THE SERVICES WILL BE UNINTERRUPTED AT ALL TIMES OR ERROR FREE.

9. **Limitation of Liability** - VV'S TOTAL LIABILITY FOR ANY AND ALL CLAIMS, WHETHER IN AN ACTION IN CONTRACT OR IN TORT, INCLUDING BUT NOT LIMITED TO, NEGLIGENCE OR STRICT LIABILITY, FOR ANY LOSS OR INJURY ARISING OUT OF, CONNECTED WITH OR RESULTING FROM VV'S PERFORMANCE OR BREACH OF THIS AGREEMENT OR THE USE, PERFORMANCE OR NON-PERFORMANCE OF THE SERVICES HEREUNDER, OR ANY PART THEREOF, SHALL NOT EXCEED THE TOTAL AMOUNT OF THE FEES PAID BY SUBSCRIBER TO VV DURING THE PRIOR THREE (3) MONTH PERIOD (OR PORTION THEREOF, IF THIS AGREEMENT HAS BEEN IN EFFECT LESS THAN THREE MONTHS) FOR THE SERVICES THAT CAUSED THE LOSS OR INJURY OR ARE THE SUBJECT MATTER OF THE CLAIM OR CAUSE OF ACTION. VV shall not be responsible for any unavailability of the Services resulting from (i) any Subscriber-ordered telephone circuits, (ii) Subscriber's applications, equipment or facilities, or (iii) acts or omissions of Subscriber.

10. **Allocation of Risk** - VV and Subscriber expressly acknowledge and agree that the limitations and exclusions contained in Sections 7, 8 and 9 of this Agreement have been the subject of active and complete negotiation between the parties and represent the parties agreement as to the allocation of risk between the parties based upon the level of risk to VV and Subscriber associated with their respective obligations under this Agreement. The payments payable to VV in connection herewith reflect this allocation of risk and the exclusion of consequential damages in this Agreement. The parties acknowledge that, but for the limitations set for in Sections 7, 8 and 9 hereof, the parties would not have entered into this Agreement.

11. **Proprietary Information and Security**

(a) Proprietary Information. Each party will regard any information provided to it by the other party as proprietary or confidential ("Proprietary Information") and each party will protect the confidentiality of the other party's Proprietary Information in the same manner as it protects its own valuable proprietary information. Subscriber expressly agrees that image enabling software, workflow enabling software, other software utilized in connection with the Services, any documentation and the terms and conditions of this Agreement are the Proprietary Information of VV (, or other third party servicer and/or consultant, as the case may be). Any copying, modification, distribution, translation, reverse engineering, reverse compiling, making derivative works or other dealing in the Proprietary Information is strictly prohibited, except to the extent deemed necessary by VV for Subscriber's use of Services hereunder. Subscriber will not remove or destroy any proprietary markings or restrictive legends placed upon or contained within any of the software or any associated documentation. Each party agrees, for itself and its agents and employees, to protect the confidentiality of any proprietary information of third parties in its possession and accepts liability for any breach of this Agreement by its agents or employees. The Services are intended for the internal use of Subscriber only. Subscriber shall not transfer, assign, distribute, re-sell, sublicense or otherwise make available the Services or access to the VV Software to any third party.

(b) Exceptions. Information will not be deemed confidential hereunder if such information: (i) is known to the receiving party prior to receipt from the disclosing party directly or indirectly, other than from a source having an obligation of confidentiality to the disclosing party; (ii) becomes known (independently of disclosure by the disclosing party) to the receiving party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing party; (iii) becomes publicly known or otherwise publicly available, except through a breach of this Agreement by the receiving party; or (iv) is independently developed by the receiving party.

The receiving party may disclose Proprietary Information pursuant to the requirements of applicable law, legal process or government regulation, provided that it gives the disclosing party reasonable prior written notice to permit the disclosing party to contest such disclosure, and such disclosure is otherwise limited to the required disclosure.

(c) Security Measures. Subscriber acknowledges the implementation of reasonable security procedures relating to Subscriber's access to the VV Software. Subscriber shall be responsible for administering the procedures relating to the assignment and administration of all identification codes and passwords authorizing access to the VV Software on behalf of or for the benefit of Subscriber, and Subscriber shall be responsible for taking appropriate security measures relating to such identification codes and passwords. Subscriber shall be solely responsible for any and all acts or omissions that occur under any account or password issued to Subscriber (and its authorized users).

(d) **Indemnification** Subscriber shall defend, indemnify, protect and hold VV and its their affiliates, shareholders, directors, officers, employees and agents harmless from and against any liabilities, actions, losses, costs, expenses (including attorneys' fees and costs) or claims incurred by any of them as a result of any misuse of the VV Software or the Services by Subscriber, its agents, employees and/or authorized users.

12. **Entire Agreement** - This Agreement, together with the Exhibits attached hereto and incorporated herein, constitutes the entire agreement of the parties with respect to the subject matter hereof, and supersedes all previous proposals, oral or written, and all negotiations, conversations or discussions heretofore and between the parties related to this Agreement. Each party acknowledges that it has not been induced to enter into this Agreement by any representation or statements, oral or written, not expressly contained herein and in any attachments, schedules, exhibits or addendums not attached hereto. The parties acknowledge that VV has set its prices and entered into this Agreement in reliance upon the limitations of liability and the disclaimers of warranties and damages set forth herein, and that the same form an essential basis of the bargain between the parties. The parties agree that the limitations and exclusions of liability and disclaimers specified in this Agreement will survive breach or termination and apply even if found to have failed of their essential purpose.

13. **Governing Law** - This Agreement will be governed by and interpreted in accordance with the laws of the State of Arizona, without regard to its conflict of laws principles. Any claims or legal actions by one party against the other arising out of the relationship between the parties contemplated herein (whether or not arising under this Agreement) shall be governed by the laws of the State of Arizona and shall be commenced and maintained in any state or federal court located in such state, and each party hereto hereby consents and submits to the exclusive jurisdiction and venue of any such court. No proceeding, regardless of form, arising out of the subject matter of this Agreement will be brought by Subscriber more than one year after the claim becomes known to Subscriber.

14. **Notices** - All notices hereunder shall be in writing and shall be delivered in person or may be sent by courier, telecopy, express mail or postage prepaid certified or registered air mail, addressed to the party for whom it is intended, at the address set forth herein.

15. **Severability** - If any provision of the Agreement is determined by a court of competent jurisdiction to be invalid or unenforceable, such provision shall, to such extent as it shall be determined to be invalid or unenforceable, be deemed to be null and void, but the remaining terms of this Agreement shall otherwise remain in full force and effect.

16. **Assignment**. Either party may assign this Agreement in whole as part of a corporate reorganization, consolidation, merger, or sale of substantially all of its assets with prior written notice to the other party. Any other assignment of this Agreement, in whole or in part, shall require the prior written consent of the other. This Agreement will bind and inure to the benefit of each party's successors and permitted assigns.

17. **Waiver and Amendment**. Any waiver, amendment, supplement or modification of this Agreement will not be effective unless set forth in writing and signed by an authorized representative of both parties. Any such written waivers, amendments, supplements and modifications will be deemed a part of this Agreement as if incorporated herein. The failure of either party to exercise any of its rights under this Agreement will not be deemed a waiver or forfeiture of such rights.

18. **Counterparts** - This Agreement may be executed in counterparts, which taken together, will constitute one Agreement, and any party hereto may execute this Agreement by signing such counterpart.

19. **Effect of Termination** - Upon the termination of this Agreement for any reason: (i) Subscriber shall be liable for all fees and any additional charges incurred prior to the date of termination and throughout any period of suspension of the Services, and (ii) Subscriber shall also be liable for all fees incurred as part of this Agreement as a result of VV's return of all Subscriber's Data, and (iii) if terminated for convenience by the Subscriber after year one of this agreement and at any time other than at the end of a Term, Subscriber must provide VV with a minimum of ninety (90) days' notice, and (iv) upon receipt of Subscriber's payment, VV will promptly return all of Subscriber's Data in VV's possession, if any, at Subscribers expense and (v) the provisions of Sections 5, 7, 8, 9, 10 and 11 of this Agreement shall survive the termination hereof. In the event either party fails to perform or observe any material covenant, condition or agreement hereunder or pay any amounts owed hereunder, then the other party may, upon 30 days' written notice, terminate this Agreement if such breach has not been cured within such 30-day period.

20. **Force Majeure** - Except with respect to Subscriber's monetary obligations hereunder, neither party hereto will be liable for any failure or delay in performance of its obligations hereunder by reason of any event or circumstance beyond its reasonable control ("force majeure"), including without limitation acts of God, war, terrorism, fire, flood, or shortage or failure of suppliers; provided, however, that for any force majeure extending for more than 60 days, the party not claiming the existence of a force majeure will have the right to give notice, pursuant to Section 14, of termination of this Agreement without penalty.

Remainder of page Intentionally Left Blank

Exhibit B - Acceptable Use Policy

VISUALVAULT Acceptable Use Policy

This Acceptable Use Policy specifies the actions prohibited by VISUALVAULT to users of the VISUALVAULT service. VISUALVAULT reserves the right to modify the Policy at any time, effective upon posting of the modified policy to http://www.visualvault.com

Illegal/Prohibited Use
The VISUALVAULT Network may be used only for lawful purposes. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

Unauthorized Uses
VISUALVAULT is intended for use only as a document storage, access, and retrieval system in support of a subscriber's or end-user's need to store, access, and retrieve documents. It is not intended for use as a temporary data or document storage and transportation mechanism or system. Documents, either individually or in volume, may not be uploaded to VISUALVAULT and then retrieved by and/or transferred to any person and shortly thereafter be deleted from VISUALVAULT. This type of activity within an VISUALVAULT account will be considered unauthorized data or document transportation and in violation of this Acceptable Use Policy under the subscriber's agreement with VISUALVAULT.

VISUALVAULT services sold on a per-Entity basis can only be utilized by a single company, enterprise, proprietorship or individual (Entity). If per-Entity services are required by or for more than one Entity, they must be purchased for each individual Entity. Per-Entity services are not authorized for use on a project-level basis that involves multiple Entities. Utilizing per-Entity services at a project level for more than one Entity, whether by a subscriber, end-user or reseller, will be considered an unauthorized use, in violation of this Acceptable Use Policy under the subscriber's agreement with VISUALVAULT.

Software Installations
VISUALVAULT may make available software to be installed by users. Any new installations of said software must be performed using the latest available version. Installing older versions of the software will be considered a violation of this Acceptable Use Policy.

System and Network Security
Violations of system or network security are prohibited and may result in criminal and civil liability. VISUALVAULT will investigate incidents involving such violations and may involve and will cooperate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

- Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network.
- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network.
- Interference with service to any user, host or network including, without limitation, mailbombing, flooding, deliberate attempts to overload a system and broadcast attacks.
- Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting.

INDIRECT OR ATTEMPTED VIOLATIONS OF THE POLICY, AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON BEHALF OF A VISUALVAULT CUSTOMER OR A CUSTOMER'S END USER, SHALL BE CONSIDERED VIOLATIONS OF THE POLICY BY SUCH CUSTOMER OR END USER.

Complaints regarding Illegal Use or System or Network Security issues should be sent to support@VisualVault.com.

Exhibit C - Support SLAs

1. **On Call Support.**

1.1.

The Principal Period of Support ("PPS") is a ten (9) hour contiguous daily time period between the hours of 8:00 AM and 5:00 PM, US Eastern Time, Monday through Friday, excluding VisualVault's published holidays.

1.2. Twenty-four (24) hour Premium Support Services are available upon request and at an additional charge. Extended coverage options are subject to VV's approval and the prevailing terms, conditions and prices for service at that time. Extended Hours Entitlement extends the Client's ability to place problem calls to VV's Technical Services Group ("TSG") during the extended hours of coverage period and receive the same priority remote response for critical issues as during the PPS.

2. **Severity Levels.**

Based on communications between Client and VV, the parties shall determine, in accordance with the following table, the "Severity Level" of each issue.

Severity Level	Definition
1	An issue that causes the Software to crash or be unavailable for use and which has no acceptable work-around.
2	An issue that affects multiple users of the Software and prevents effective use of an essential feature or essential features of the Software, but which does not cause the Software to be unavailable for use in whole.
3	An issue that affects productivity or ease of use of the Software and for which there is typically a work around.
4	An issue that does not materially affect Client's (or any Client Customer's) ability to use the Software (e.g., user interface inconveniences).

Based on the "Severity Level" of the issue, each of VV and Client shall take the following actions:

Severity Level	VV Responsibilities	Client Responsibilities
1	Acknowledge and begin addressing immediately. VV's Client support and production support teams will work continuously until fixed, 24x7 if not resolved by the close of the business day. Such 24x7 effort	Call at time of discovering issue (email not acceptable for Severity 1). Be available to answer questions, provide information, and receive and install code fix immediately, 24x7 if not resolved by the close of the business day.

	to commence first business day after determination of severity. Target resolution time is four (4) hours.	
2	Acknowledge and begin addressing promptly. VV's Client support and production support teams will work continuously within normal business hours until resolved. Target resolution time is 24 hours.	Be available to answer questions, provide information within four (4) hours of request. Install/test fix providing feedback.
3	Acknowledge within one business day. Issue will be scheduled to be addressed, based on the priority set by Client and VV. Target resolution time is seven (7) days.	Provide information and answer questions within one (1) business day.
4	Acknowledge within one business day. Issue will be addressed when possible, based on the priority set by Client and VV.	Provide information and answer questions within three business days.

TAB 3

NEBRASKA

Good Life. Great Mission.

DEPT. OF HEALTH AND HUMAN SERVICES

- Create the New Normal
- Transform Service
- Transform Outcomes

TAB 3

TECHNICAL APPROACH

The VisualVault Aging Information System Platform creates the New Normal and renewed excitement for all as the ability to deliver improved outcomes for seniors becomes the reality.

UNDERSTANDING PROJECT REQUIREMENTS

The bidder should provide the following information in response to this RFP:

PROJECT OVERVIEW

The importance of the programs and oversight Nebraska's Aging Information System provides Nebraska senior residents is an imperative based on the size of this population in the state, The strategic decision to modernize the enterprise client Information Management System (AIS) is a mission critical step towards improving the structure around service assessment/delivery requirements.

VisualVault understands the unique nature of NE's aging program. NE's aging population are arguably the most vulnerable among us and the department has the privileged responsibility to assure the services each requires are delivered efficiently, accurately, and with compassion. The aging population is rapidly expanding, the diversity of the population continues to grow, and Nebraskans want consumer directed alternatives to nursing home care. Nebraska coordinates multiple agencies to promote the current efforts on aging and provide services to this population. The state agencies coordinate funds from federal, state, and private sources to deliver services to aging citizens. From your multi-year plan, we understand the strategies, objectives, and measurements used to coordinate the programs. The VisualVault AIS platform will play a vital role in assisting DHHS to coordinate and administer these programs to this rapidly growing population.

VisualVault was recently selected to deliver a Marijuana Registry and a Child Services System--continued proof of the flexibility of this unique platform and the value of Community Licensing.

The "New Normal" for Client Interactions and Overall Program Management

VisualVault proposes an innovative approach to automate and modernize State Unit on Aging (SUA) operations. The VisualVault SaaS platform and unique pricing model is a positive disruptive influence for state departments to transform the way staffs interact and collaborate with elders and supporting program partners. VisualVault introduced this innovative approach to improve quality service delivery by recognizing a phenomenon in state business processes associated with "external" users. There exists an artificial barrier to equal access to software use. The phenomenon exists not because of a technical deficiency, but rather because traditional software licensing uses the number of users as the basis for the price. Concurrent and Named user pricing created the unexpected consequence of the two-tiered user community. Staffs and select "internal" users gained benefits from new software functionality while those being served, service providers, supporting organizations/partners remained excluded and forced to complete work and communicate with departments using 1980's communication models of blind portals and email attachments. Even SaaS pricing introduced in 1999 and made popular by Salesforce is based on a per user basis. This two-tiered model negatively impacts the entire user community and limits the potential for SUA new AIS.

The challenge for SUA staff is the need to interact, communicate, and process inbound data and support documentation from AIS users and support community. Concurrent and named user licensing restricts system use to internal SUA users. VisualVault asked the question, "How effective is it to limit use compared to the benefits of extending system use to all service providers, caregivers, and elders themselves?" VisualVault's Community Licensing transforms the outdated approach of restrictive use by creating an interconnected digital highway with unlimited on-ramp access for all participant. The *New Normal* will be a completely transparent, structured Client Management System that engages the

whole community of participants to perform their work easier, faster, and with complete transparency by working directly within the Aging Information solution. The breakthrough occurs because VisualVault's Community Licensing, licenses by the program and all supporting processes, NOT by the number of users.

The combination of our understanding of SUA's requirements and goals, single/flexible/configurable platform, Community Licensing that extends direct system access to all and the right experience working directly with the software provider contribute to best overall value.

DELIVER FLEXIBLE FUNCTIONALITY THAT MEETS TODAY'S REQUIREMENTS AND THOSE NOT ON YOUR RADAR....

The VisualVault implementation approach and SaaS platform makes the client Aging Information System (AIS) the system of record for all client management information.

Configuring functionality: Core code is never altered to create customized functionality. AIS is designed to have functionality configured for each implementation. Forward-thinking design enables VisualVault Team to cost effectively deliver all required AIS functionality and the platform flexibility will provide for continued tweaking as requirements evolve and change.

No Need to integrate multiple software to create the AIS. With VisualVault, there is no need to increase project risk with integrating multiple applications to deliver the required functionality. All proposed aging information functionality is inherent to the VisualVault platform. This benefit reduces the risk to the project, reduces costs, enables our delivery team to work on the same technology to gain the repetition that brings accuracy and speed to successful implementations.

Complete oversight and audit capability: VisualVault was originally developed as a compliance solution for auditing medical record manufacturers. Every touch within and to the platform, change, activity and action is recorded and will be used to create reporting and audit trails SUA needs to comply with all State and Federal requirements.

Organizational Change Management, a large risk area often overlooked. Stephenie Colston is an important part of our team to address the need for training excellence. With twenty-five years' experience managing organizational training and documentation efforts at Federal, State agency, community provider, and hospital levels, Stephenie's government experience will prove to be invaluable. VisualVault recognizes the importance of training and assigns the highest level of talent to provide the strategy, plans and reports to assure this project is successful.

CASE MANAGEMENT

VisualVault's AIS is built on top of a compliance and enterprise content management automation platform. The platform is designed to manage and track all actions associated with a file or case. iForms are configured to provide the vehicle for a complaint or assertion of improper events/actions/activities associated with an individual or group. Workflow auto routes the initial information to the right person for review. Triaging initial case information is easily completed as all involved have direct access to the information to make the determination. When a complaint is deemed valid, the AIS platform auto generates a unique case number and assigns it to the case's iForm cover sheet. The compliant iForm becomes the case "cover sheet." All subsequent documentation, notes, photos, etc. as linked to the case. Notifications, meeting schedules, assessment forms, etc. are all components of the AIS automated case management system. When changes occur, old value and new values are recorded in a change log. When users complete tasks, view the complaint/referral or change data, the events are recorded. The SUA and partners have complete visibility into each action and interaction conducted. Reports are built using the log data to provide management with the KPI information needed to manage and oversee staff and processes. Dashboards also are used to show KPI information in real-time. With Community Licensing, all users have secure access to see their portion or the entire case based on security credentials.

DASHBOARD VIEW OF OPEN CASES

EXPERTISE IN DATA MIGRATION

Data Migration is the second risk area for project success. VisualVault identified the complexity of SUA's data migration. A determining factor to partner with ProCom Consulting is their extensive experience with large, complex data migration project. They have the experience and tools to assure this requirement is completed successfully.

VisualVault teamed with ProCom Consulting (ProCom) to provide integration services, particularly focused on integration of internal and external systems, data migration, and providing strong project management with local, Florida-based project management.

ProCom's senior management consists of highly experienced consulting professionals with background from leadership and delivery in large "Big Six" consulting practices. This means that ProCom consistently brings the practices, discipline and experience that are consistent with the quality and consistent delivery practices of the world's largest systems integrators.

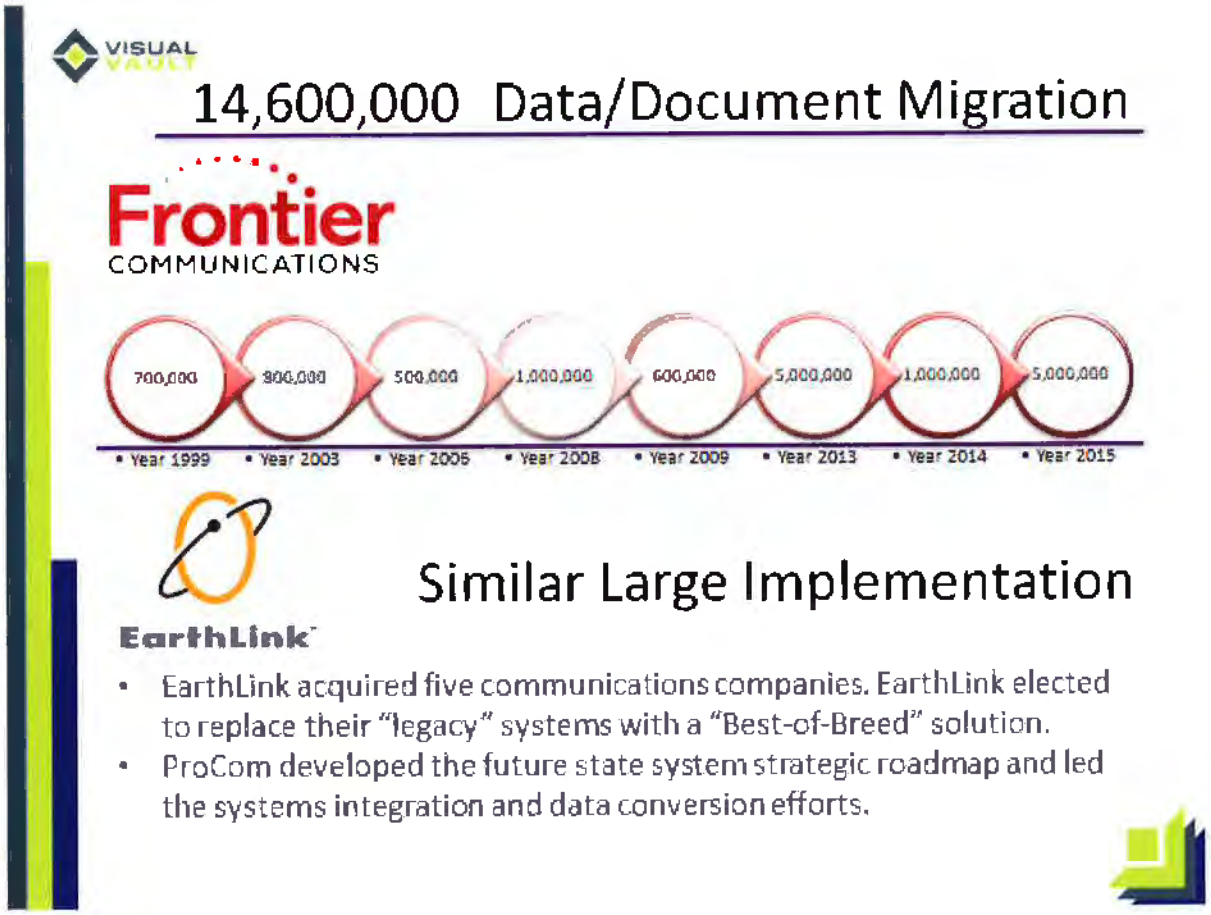
Founded in 1999, ProCom Consulting provides Information Technology resources to help clients achieve mission critical projects. ProCom Consulting supplies experienced professionals to support applications development, data strategy and management, quality assurance, technology research, client technologies, customer support, network management, Internet planning and operations, data center operations, telecommunications, electronic commerce, business intelligence, ERP, sourcing, vendor management, business management, training, security management, systems continuity, product development, systems programming, business analysis, release management, program management, customer service, and technical product support.

ProCom is trusted by commercial and government organizations with their mission critical projects including large technology projects, complex organizational transformations, merger integration support, application maintenance and development, and ongoing operations. Through nearly two decades of merger integration support in the telecommunications industry, ProCom has developed and honed particular areas of focus on Project Management of large projects involving complex data migration and multiple systems interfaces. ProCom has supported Frontier Communications for almost twenty years as they tripled in size. ProCom supported Frontier as they acquired other companies and merged millions of customers into their business operations, application systems and databases. Frontier has turned to ProCom for over 15 projects to manage this large scale merger support.

ProCom currently employs 200 consulting staff and has demonstrated capability to scale projects ranging from 1 to 100 staff. Since inception, ProCom Consulting has provided over 15,000 consulting resources in support of our clients' mission critical work, with total contract values in excess of $130 million. ProCom services range from full project delivery responsibility to providing individual resources where needed to complement clients' own internal team. ProCom has honed personnel practices and

employment processes to quickly locate and mobilize the right resources to meet client needs. ProCom has a vast database of existing personnel and candidates, as well as strong relationships throughout the industry, which enable them to locate the best resources.

ProCom is headquartered in Atlanta, Georgia and maintains a staffed office location in Tallahassee, Florida. For this project, ProCom's team includes staff with more than 30 years of insurance experience including more than 10 years of Property & Casualty specific experience, managing projects that include integration with the Guidewire software suite and several other of Citizens' software solutions, as well as working directly with the Department of Financial Services' Division of Agent and Agency Licensing and their system of record for Agent and Agency licenses and appointments.



OMBUDSMAN FUNCTIONALITY INCLUDED

The VisualVault Team understands the importance of the Ombudsman services. Based on the fact that they are a part of the community of users who contribute to elder services, we include them (at no additional charge) in our Community Licensing fee. The VisualVault Team realizes that DHHS did not provide functional details for this group. Therefore, there will need to be discovery work to determine how best to incorporate their processes into the overall program design. We have included some leeway in our implementation pricing to provide what we expect are basic functions.

We have included Licenses for the Ombudsman group based on their importance to the program at no additional cost

SCOPE OF WORK REQUIREMENTS

TECHNICAL REQUIREMENTS
FUNCTIONAL REQUIREMENTS
The proposed System must meet the Business Requirements per Attachments B
SYSTEM USERS
The solution must allow for 150 to 250 users across the SUA, IS&T team, and AAA teams to access the current system without negatively impacting performance.

THE VISUALVAULT DIFFERENCE: COMMUNITY LICENSING

The VisualVault team is not proposing an Aging and Information system based on the old model constrained by legacy software licensing. VisualVault is proposing a transformative model where all stakeholders benefit -- at a lower investment. These benefits are possible because VisualVault licenses our SaaS aging information platform based on the NE SUA program and supporting processes, NOT by the number of concurrent or named users. The benefits of Community Licensing is everyone contributing to the betterment of elder services is provided a user license that enables them to have complete transparency into all actions and activities.

From a strategic position, Community Licensing promotes internal and external users to work collaboratively within the platform reducing caseload work. Community Licensing eliminates artificial barriers and "workarounds" driven by the need to comply with restrictive software licensing requirements that create two classes of users: those few with access to the full functionality of the software and reports (the "Haves") and those who have either no or only very limited access (the "Have Nots"). The VisualVault team proposes the solution to eliminate the negative effect the "Have and Have Not" licensing barrier presents to NE DHHS and partner's user community. When you change the scenario where all users have secure log in credentials and are verified to work directly in the VisualVault system -- the paradigm shifts in the level of accuracy and speed of reporting, service, responsiveness, self-service, and ease of use.

Community Licensing enables DHHS to replace AIS with the next generation platform with a single low-cost software platform, configurable to:

1. Replace of the current agency developed software
2. Establish case management and services for aged and disabled clients
3. Setup an Information & referral database for employee and public use; and
4. Provide Ombudsman the Access they require to provide a more integrated approach to long term care with one single platform

Community Licensing engages all community users to work collaboratively within the system for the benefit of the seniors served for a one low flat annual fee.

SYSTEM PRIVACY
The solution must comport with all applicable laws and regulations regarding privacy, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA), and the provisions contained in the Business Associate Agreement Provisions - Attachment

In the provision of any service under this contract, the Contractor must comply with all applicable law, including but not limited to federal and state: statutes, rules and regulations, and guidance documents. Compliance includes, but is not limited to:

The Health Information Protection and Portability Act (HIPAA), as set forth in Attachment F; and

The Medicaid-specific above-and-beyond-HIPAA privacy protections found at 42 CFR Part 431, Subpart F

Attachment P GRM VisualVault Encryption and Key Management
Attachment A GRM VisualVault 2016 Type 2 SOA 2 Final Report
Attachment B GRM VisualVault HIPAA-HITECH Security Assessment - Final Report
Attachment C GRM VisualVault Support for HIPAA Compliance

HARDWARE AND SOFTWARE REQUIREMENTS
The State requires a solution where all hardware and software are hosted and maintained by the contractor.
HARDWARE
The bidder must provide all necessary hardware, systems software (operating systems licenses, auxiliary or support systems software, etc.) and disk storage space required to optimally effect the solution. The solution offered must take into consideration storage requirements over the entire contract term, including all optional renewal and extension periods. The solution must consider the State's records retention requirements. Below is the link to AAA records: http://www.sos.ne.gov/records-management/pdf/156%20-%20NE%20Area%20Agencies%20on%20Aging%20WEBSITE%204-5-11.pdf
And below is the link to the DHHS, MLTC, SJA records: http://www.sos.ne.gov/records-management/pdf/150-3-7-medicaid-long-term-care.pdf
SOFTWARE VERSIONS
The contractor will, during the entire contract, maintain any and all third-party software products at their most current version and no more than two (2) versions back from the most current version at no additional cost to the State. All security patches for the software must be applied and kept up to date.

VisualVault has read and accepts the requirements for hardware and software.

PROJECT PLANNING AND ANALYSIS PHASE

The following table contains the list of requirements and due dates expected of the contractor for the Planning and Analysis phase of the project. Details for these requirements follow in the text after the table.

	Phase	Requirements	Due Date
1.1	1.0 Project Planning	Draft Project Work Plan	Submitted with Proposal
1.2		Detailed Project Work Plan	Due 2 weeks after Contract Start Date
1.3		Testing Methodology	Due 2 weeks after Contract Start Date
1.4		Project Control Documents Risk Management and Resolution Plan Issue Management and Resolution Plan Organizational Change Management Plan Work Management Plan Change Control Documents	Due 2 weeks after Contract Start Date
1.5		Status Reporting Plan Project Status Meeting Protocol	Due 2 weeks after Contract Start Date
1.6		Electronic Project Library	Due 2 weeks after Contract Start Date

1.7		Security Plan	Due 2 weeks after Contract Start Date
1.8		Business Continuity Plan/Disaster Recovery Plen	Due 2 weeks after Contract Start Date
2.1	2.0 Requirements Analysis	Requirements Validation Document (RVD)	Due dates to be determine d in the Deteiled Work Plan
2.2		Fit/Gap Analysis	Due dates to be determine d in the Detailed Work Plan
2.3		Pilot/Prototype	Due dates to be determine d in the Detailed Work Plan

We have assumed the Pilot/Prototype, as part of the Requirements Phase, will act as a demonstration of the desired functionality. We did not assume this prototype would be equivalent to the production system, nor will there be a data conversion from the legacy system to allow users to practice using this version of the solution. It will be an illustration of the final product that will integrate all the requirements defined.

VISUALVAULT'S DRAFT PROJECT MANAGEMENT SCHEDULE

Deliverable Overview

Task Name	Duration	Start	Finish
NE Aging Information System Software Solution	**171.96 days**	**Fri 3/1/19**	**Fri 11/1/19**
Contract Execution	1 day	Fri 3/1/19	Fri 3/1/19
Project Planning - Project Management	**156.28 days**	**Mon 3/4/19**	**Fri 11/1/19**
Requirements Analysis - Deliverable 2	**38.63 days**	**Mon 3/11/19**	**Thu 5/2/19**
Design - Deliverable 3	**12.42 days**	**Mon 4/1/19**	**Thu 4/18/19**
Configuration / Development - Deliverable 4	**93.25 days**	**Tue 4/2/19**	**Tue 8/13/19**
Data Conversion / Migration (Deliverable 5)	**126.81 days**	**Thu 3/14/19**	**Thu 9/12/19**
Testing - Deliverable 6	**26.76 days**	**Mon 8/26/19**	**Thu 10/3/19**
Training - Deliverable 7	**23.75 days**	**Mon 8/26/19**	**Mon 9/30/19**
Data Migration/Integration - NE "Implementation" - Deliverable 8	**142.81 days**	**Thu 4/11/19**	**Fri 11/1/19**

VISUALVAULT'S DRAFT PROJECT MANAGEMENT SCHEDULE
High-Level Overview

Task Name	Duration	Start	Finish
NE Aging Information System Software Solution	**171.96 days**	**Fri 3/1/19**	**Fri 11/1/19**
Contract Execution	1 day	Fri 3/1/19	Fri 3/1/19
Project Planning - Project Management	**170.09 days**	**Mon 3/4/19**	**Fri 11/1/19**
Project Management - Initiation	**16.63 days**	**Mon 3/4/19**	**Tue 3/26/19**
Quarterly Project Management	**66 days**	**Mon 3/18/19**	**Wed 6/19/19**
Quarterly Project Management	**61 days**	**Mon 6/24/19**	**Thu 9/19/19**
Project Management – Close-Out	**26.34 days**	**Tue 9/24/19**	**Fri 11/1/19**
Requirements Analysis - Deliverable 2	**38.63 days**	**Mon 3/11/19**	**Thu 5/2/19**
Discovery	**3.5 days**	**Mon 3/11/19**	**Thu 3/14/19**
Requirements Specifications	**28.5 days**	**Fri 3/15/19**	**Thu 4/25/19**
Form specifications	**10.87 days**	**Mon 3/18/19**	**Mon 4/1/19**
Business logic & validation script specifications	**1.5 days**	**Mon 3/18/19**	**Tue 3/19/19**
Report specifications	**2.05 days**	**Mon 3/18/19**	**Wed 3/20/19**
Search specifications	**0 days**	**Fri 3/15/19**	**Fri 3/15/19**
UI (portal screen) specifications. 6 Roles	**0.38 days**	**Mon 3/18/19**	**Mon 3/18/19**
Requirements Validation Document	**13.25 days**	**Mon 4/1/19**	**Fri 4/19/19**
Fit / Gap Analysis	**13.25 days**	**Mon 4/1/19**	**Fri 4/19/19**
Requirements Specifications Document	**7.29 days**	**Mon 4/1/19**	**Thu 4/11/19**
Pilot / Prototype	**17.64 days**	**Mon 4/1/19**	**Thu 4/25/19**
Acceptance	**5.13 days**	**Thu 4/25/19**	**Thu 5/2/19**
Design - Deliverable 3	**12.42 days**	**Mon 4/1/19**	**Thu 4/18/19**
Detailed System Design Documentation	**7.29 days**	**Mon 4/1/19**	**Thu 4/11/19**
Testing Plan	**6.79 days**	**Mon 4/1/19**	**Wed 4/10/19**
Acceptance	**5.13 days**	**Thu 4/11/19**	**Thu 4/18/19**
Configuration / Development - Deliverable 4	**93.25 days**	**Tue 4/2/19**	**Tue 8/13/19**
4.1 Plan, Schedule, Environment Set-Up	**8.58 days**	**Tue 4/2/19**	**Mon 4/15/19**
Development / Customization	**74 days**	**Thu 4/11/19**	**Fri 7/26/19**
4.2 Core Processes	**14 days**	**Thu 4/11/19**	**Wed 5/1/19**
4.3 Client Services - CLI-1 to CLI-18	**10 days**	**Mon 4/29/19**	**Mon 5/13/19**
4.4 Services - SER-1 to SER-19	**10.42 days**	**Thu 5/9/19**	**Thu 5/23/19**
4.5 Assessments ASMT-1 to ASMT-14	**15.77 days**	**Wed 5/22/19**	**Thu 6/13/19**
4.6 Usability USE-1 to USE-13	**5.04 days**	**Wed 6/12/19**	**Wed 6/19/19**
4.7 Fiscal FIS-1 to FIS-9	**5.63 days**	**Fri 6/14/19**	**Fri 6/21/19**
4.8 Reporting REP-1 to REP-15	**13.67 days**	**Thu 6/20/19**	**Wed 7/10/19**
4.9 Volunteer Management VOL-1 to VOL-2	**3.52 days**	**Thu 7/11/19**	**Tue 7/16/19**
4.10 Provider Information PRV-1 to PRV-5	**3.38 days**	**Mon 7/15/19**	**Thu 7/18/19**
4.11 Operations OPR-1 to OPR-7	**7 days**	**Wed 7/17/19**	**Fri 7/26/19**
4.12 Reports / UI	**3.83 days**	**Fri 7/26/19**	**Wed 7/31/19**
4.13 Configuration Close-Out	**78.79 days**	**Tue 4/23/19**	**Tue 8/13/19**
Data Conversion / Migration (Deliverable 5)	**126.81 days**	**Thu 3/14/19**	**Thu 9/12/19**
Data Conversion Plan & Guide - 5.1	88.87 days	**Thu 3/14/19**	**Fri 7/19/19**
Data Conversion Environment - 5.2	**17.42 days**	**Wed 7/31/19**	**Mon 8/26/19**
Conversion Results Report - 5.3	**6.79 days**	**Mon 8/26/19**	**Thu 9/5/19**

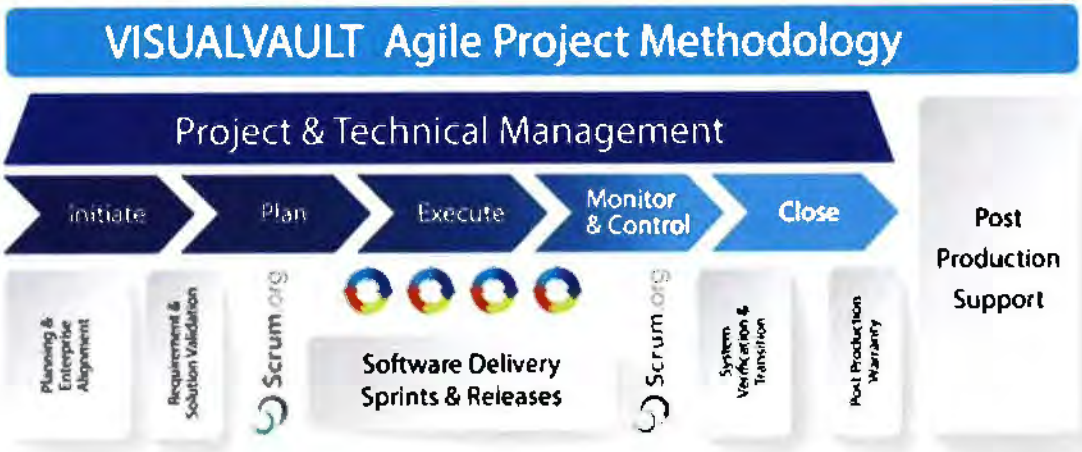
Acceptance	**5.13 days**	**Thu 9/5/19**	**Thu 9/12/19**
Testing - Deliverable 6	**26.76 days**	**Mon 8/26/19**	**Thu 10/3/19**
Unit, System, Interface Test Plan - 6.1	**1.99 days**	**Thu 9/5/19**	**Mon 9/9/19**
Conduct Unit Testing	11.96 hrs.	Mon 9/9/19	Tue 9/10/19
Conduct Internal System Testing	11.96 hrs.	Tue 9/10/19	Thu 9/12/19
Conduct Interface Testing	11.96 hrs.	Thu 9/12/19	Fri 9/13/19
User Acceptance Plan & Testing	**26.76 days**	**Mon 8/26/19**	**Thu 10/3/19**
UAT Plan - 6.1	**16.5 days**	**Mon 8/26/19**	**Wed 9/18/19**
Testing - 6.2	**3.13 days**	**Wed 9/18/19**	**Tue 9/24/19**
Acceptance	**7.13 days**	**Tue 9/24/19**	**Thu 10/3/19**
Training - Deliverable 7	**23.75 days**	**Mon 8/26/19**	**Mon 9/30/19**
Training Plan (4 strategies, 2 approaches) - 7.1	**7 days**	**Mon 8/26/19**	**Thu 9/5/19**
Training Documentation	**3.75 days**	**Mon 8/26/19**	**Fri 8/30/19**
Conduct Training Sessions	**14.88 days**	**Fri 8/30/19**	**Mon 9/23/19**
Training Manual - 7.4	**1.79 days**	**Thu 9/5/19**	**Mon 9/9/19**
Acceptance	**5.13 days**	**Mon 9/23/19**	**Mon 9/30/19**
Data Migration/Integration - NE "Implementation" - Deliverable 8	**142.81 days**	**Thu 4/11/19**	**Fri 11/1/19**
Implementation Plan - 8.1 - includes Problem Resolution Plan	**69.34 days**	**Thu 4/11/19**	**Fri 7/19/19**
Integration / Interfaces - 8.2	**16.87 days**	**Fri 7/19/19**	**Tue 8/13/19**
Data Migration - 8.3	**33.53 days**	**Tue 8/13/19**	**Mon 9/30/19**
Test Migrations (Mock Data Conversion Iterations)	72.22 hrs.	Tue 8/13/19	Mon 8/26/19
Migrations	5.12 days	Mon 8/26/19	Tue 9/3/19
Final Readiness Assessment (Checklist)	**0.25 days**	**Tue 9/24/19**	**Tue 9/24/19**
Deployment to Production	19 hrs.	Thu 9/26/19	Mon 9/30/19
System Go-Live	0.5 days	Mon 9/30/19	Mon 9/30/19
Documentation - 8.4	**10.94 days**	**Mon 9/30/19**	**Wed 10/16/19**
Acceptance	**12.13 days**	**Wed 10/16/19**	**Fri 11/1/19**

Note: Blue text in the above schedule delineates a deliverable. Green text delineates a work product.

PROJECT PLANNING (1.0)

The State requires that each bidder has established project management processes and has integrated these into its organizational culture and projects of similar scope and size. Proven methodologies and standards, used to control all project activities, are crucial to the success of this project. The State is not dictating a specific methodology or approach; it prefers that the bidder use an approach that has proved successful in the past. However, DHHS reserves the right to mandate the approach be revised if it does not result in the completion of timely and quality project deliverables, or it affects the project's success.

The VisualVault's approach to project management is based upon our combined experience with similar State projects focused on the improvement of key processes.
VisualVault relies on a combination of Agile Project Methodology (APM) and detailed up-front planning, common today for the delivery of enterprise COTS solutions. This methodology has been used by The VisualVault Team and has proven highly successful on implementation projects of similar size and scope. APM is aligned with industry leading standards such as the Project Management Institute's Agile Certified Practitioner (PMI-ACP) and demonstrates our commitment to using best practices for project management, software implementation, and software documentation. The illustration below illustrates our balanced approach:



The VisualVault Team's initial project planning is designed to leverage AIS' business and technical expertise already in place. Building a strong partnership with your team members is critical to the success of the project. Additionally, this approach establishes the strong communication channel between VisualVault and the DHHS teams from the beginning and facilitates delivery of processes in an efficient manner.

The VisualVault Team's project plan will incorporate project planning, enterprise alignment, as well as a Waterfall/Agile implementation approach. The methods for each are intertwined and once the initial planning stage is set the individual processes and data integration project lend themselves to this hybrid methodology nicely.

All VisualVault projects follow a Project Closure Process to continuously harvest the experience and best practices from across the organization and use it to continuously refine the standard processes and enhance the methodology. VisualVault's configurable core and reusable iForm and correspondence templates enable the delivery team to hit the ground running, bring lessons learned and industry best practices to your project.

WATERFALL/AGILE PROJECT MANAGEMENT

The VisualVault Team starts with a Waterfall model to enable us to gain and document the functionality during the Discovery phase. During this phase of the project, we meet with subject matter experts, project stakeholders and customer leadership to understand the needs of the organization, the business processes, roles of individuals involved in the process, security and reporting needs. We seek to identify issues and bottle necks in the current process. We seek to suggest solutions to resolve current issues. We then develop a specifications document that outlines how the system will be configured to meet the needs and scope of the project.

The VisualVault Team includes Mark Ervin former FL Department of Persons with Disabilities CIO. Mark managed a similar system modernization project in 2015. Mark will be intimately involved in the JAD sessions contributing his experiences to help us avoid potential pot holes in the road.

As part of project implementation using SCRUM, The VisualVault Team divides the application configuration, delivery and development tasks into single processes. The implementation of each process may build upon previously completed processes. Process dependencies and re-use are taken into consideration during the initial planning stage and a key reason as to why this hybrid approach is most efficient as many configurations can be reused to speed delivery.

Configuring processes one at a time, provides maximum focus on the tasks at hand and enables the teams to respond to feedback and change, building exactly and only what is needed. It also provides DHHS with a transparent view of what is being configured over the entire course of a project, rather than a sudden (and often fatal) revelation at project's end. This approach has been empirically proven to provide the best Return of Investment.

The VisualVault team plan is to work with business SMEs and staff to understand each process and then divide work into iterative work cycles (Sprints) that are typically 7-21 days. In Sprint planning sessions, each cycle is broken down to a manageable number of processes or milestones to work on to assure that Sprints are divided into manageable pieces.

Processes may consist of applications, assessment reports, deficiency/corrective action plans, real-time dashboards, reports and output documents (notifications and correspondence), interfaces and product/process documentation produced by the Sprint Team.

Processes also include component features and functions, and Sprint tasks are validated, executed, and demonstrated at this level. Our goal is to deliver production ready software and processes that are demonstrated and tested with each sprint. These short cycles ensure that the team gets constant feedback and course correction from the process owners and SMEs, who confirm the processes defined at the start of a project.

To deliver the required solution, we will structure process releases. Each release is decomposed into Sprints, with each Sprint resulting in demonstrable processes. Our sprint methods are summarized below.

Requirements and Validations

During the planning, requirements and validation phase, we will take the time to understand an overview of all current processes and how they work together as a complete system.

Additionally, the discovery process focuses on the outcomes requires "looking forward" opposed to myopically looking to the past. The VisualVault Team will peg each outcome and collaboratively work with the DHHS team members to work backwards from the outcome to develop your new automated processes.

Requirements planning relies on a thorough discovery of each process through meetings with team owners and examination of current data. At this stage, it's critical to identify assets that can be leveraged for this project. Once an overview of all processes has been defined, we will prioritize, with the approval of DHHS staff, priorities for the processes to deliver. We will then develop and prioritize user acceptance test plans with process owners. Our combined VisualVault and Sprint teams review

the updated test plans and work to validate acceptance criteria. The Sprint team commits to the Process Owner an achievable scope given the Sprint duration. Once an agreement is reached in the planning meeting, the Sprint team begins Sprint Execution.

Sprint Planning Process

As part of the planning process, statement of work and sprint plans for each phase are documented. This maintains traceability and provides a variety of benefits for tracking and reporting project metrics including status. Details of our planning process are summarized below.

Creation of Statement of Work by Process

We meet with team(s) and create a statement of work based on your RFP requirements. This includes each process team owner, subject matter experts and project managers. "Current state" processes are discussed, "future state" directions are reviewed, if applicable integration for inbound and/or outbound data is discussed as well as any data migration requirements.

The VisualVault team then documents the desired process in detail and submits to the team for approval. The planning sessions provide the core of the SOW therefore it is anticipated that the process owners will uncover relatively minor changes but in some cases processes owners may identify significant deficiencies. Identifying deficiencies prior to effort being put forth is critical to avoid delays.

User Acceptance Testing by Process

As processes are delivered the Process Owners will develop test plans and execute them with the assistance of the VisualVault team. This is critical to the communication process and the ultimate success of any project relies on the process improvement for the business owner and their constituents. After testing and review the process is either approved or reviewed with corrective action.

Documentation by Process

Once the UAT has been accepted by the Process Owner(s) then final documentation is created defined by each specific process. This will include agreed upon functionality and usage specifically the responsibility of the DHHS as previously agreed upon in the initial project scope.
The VisualVault Team project planning and delivery approach is designed to deliver:

- A focus on the process improvement for business value
- Delivery quality with everything we do
- Make it easy for the team to collaborate and provide status updates
- Communicate release, sprint and overall project status transparently and in a timely manor

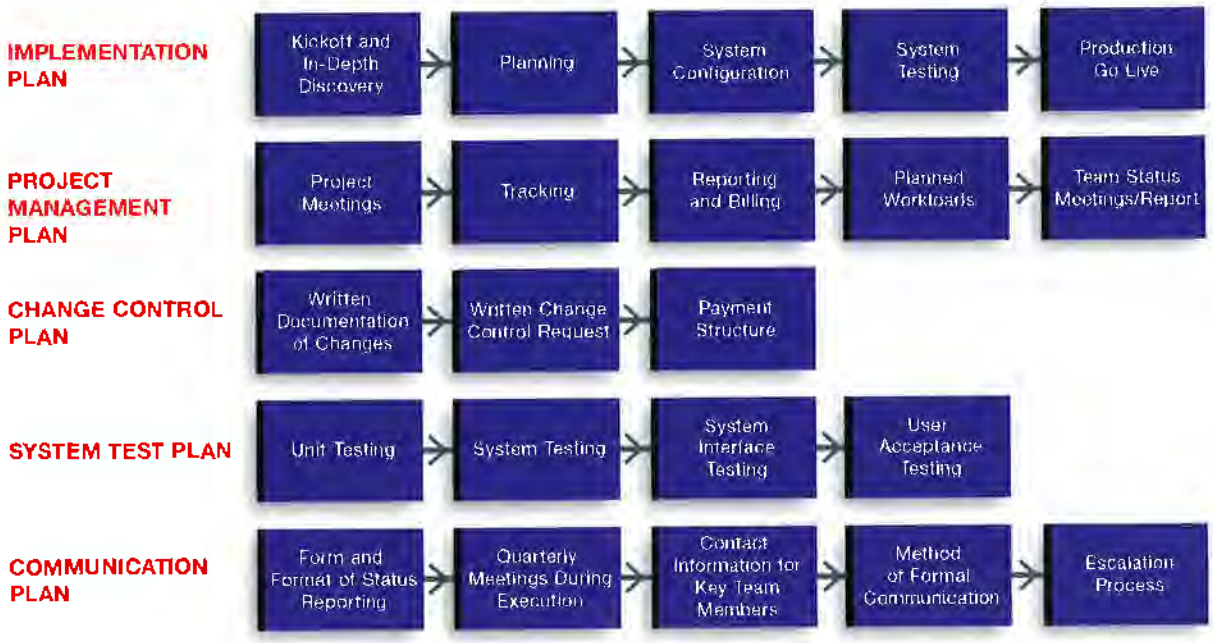
Our hybrid methodology to project planning and release/sprint planning provides a right-sized, right tool approach that provides sponsors and product owners with a quality and accurate program level status, and the project and sprint teams with tactical release and spring status.

Delivery and Training

Our Sprint cycles are designed to accelerate preliminary user acceptance testing and the preparation of system and training documentation. Our goal is to deliver process improvement with each Sprint, complete with training and system documentation with the enthusiast support of process owner support team. After each Sprint is concluded, we conduct the traditional Sprint closure activities such as retrospectives, process updates, review, and overview of impediments with the Process Owner.

In summary, The VisualVault Team's plan to deliver process improvements for follows our experience leveraging a hybrid Waterfall/Agile approach based on industry standards and our success with this methodology.

VISUALVAULT PLANNING SWIM LANES



DRAFT PROJECT WORK PLAN (SUBMITTED WITH PROPOSAL) (1.1)

Integral to the success of the project is a solid project plan and the management of that plan. The bidder shall prepare a Draft Project Work Plan to be submitted with its Proposal. The bidder shall develop a viable Project Plan that meets contractual requirements and timelines with the timing necessary for successful pre-implementation activities.

VisualVault has provided the plan and is in compliance with this requirement.

DETAILED PROJECT WORK PLAN (1.2)

Within two (2) weeks from the contract start date, the contractor will develop a Detailed Project Work Plan that includes a schedule and Gantt chart (for all project tasks, subtasks, and activities), milestones, and Detailed Project Work Plan deliverables. Resources from the contractor and the number and type of DHHS staff needed must be included for all tasks, subtasks, and activities that exist as line items within the Detailed Project Work Plan. The contractor's Project Work Plan will also maintain the following date-sensitive information:
Originally scheduled Start and End dates for all tasks, subtasks, and activities (including milestones and deliverables)

The VisualVault Team has read and will comply with this requirement.

TESTING METHODOLOGY (1.3)

The contractor must present methods for developing and maintaining test scenarios, test sets, test cases, and test steps. Testing Methodologies must also address the contractor's approach to documenting test procedures and test results.

The VisualVault Team will provide comprehensive test plan and testing. The Plan shall be reviewed and accepted by the DHHS project team. The plan shall provide an overview of the testing strategy for the system as well as plans for unit testing, system testing and user acceptance testing. Individual software components will be thoroughly tested, both at the unit and system level prior to delivery to for user acceptance testing. In the case of failure and corrections, regression testing techniques will be used to validate full functionality. Documentation of such testing will be presented before DHHS accepts system components for User Acceptance testing. The Testing Plan will address, at a minimum, the following key testing activities:

A. Unit testing: Unit testing will be performed using pre-defined test scripts that cover all the functionality of the VisualVault platform being tested.

- Unit testing scripts: Unit test scripts will be created in conjunction with DHHS Subject Matter Experts (SME) having expert knowledge of the process(s) and data being tested.

- Unit testing sign-off: Unit testing evaluation and sign-off is required by the VisualVault team. Completed unit test results shall be presented to DHHS' as part of project documentation and prior to commencing any system or user acceptance testing.

A. **System testing**: System testing, including testing mobile compatibility will be performed using pre-defined test scripts that cover all the functionality of the overall system components being tested. System testing will be accomplished by the VisualVault team from within DHHS' environment.

- System testing scripts: System test scripts will be created in conjunction with DHHS SME's having expert knowledge of the processes being tested. The system testing scripts will include tests for mobile compatibility. All test scripts will be approved by DHHS project team prior to their execution.
- System testing sign-off: System testing evaluation and sign-off is required by the VisualVault team. Completed system test results shall be presented to DHHS as part of project documentation and prior to commencing any user acceptance testing.

B. **System interface testing:** System interface testing will be performed. System interface testing shall be accomplished by the bidder team from within the DHHS environment.

- System interface testing scripts: System interface testing will be created in conjunction with DHHS SMEs having expert knowledge of the systems and data being tested. System interface testing will include end-to-end tests verifying the completeness and timeliness of all data exchanged between systems. All test scripts will be approved by the DHHS project team prior to their execution.
- System interface testing sign-off: System interface testing evaluation and sign-off is required by the VisualVault team. Completed test results will be presented to DHHS prior to activation of the interface.

C. **User acceptance testing:** User Acceptance testing shall be performed, first, within DHHS' Testing Environment and then, upon approval from DHHS, within DHHS' Production Environment. All User Acceptance testing will be performed by designated DHHS SMEs.

- User acceptance testing scripts: User acceptance testing scripts will be created in conjunction with DHHS SMEs having expert knowledge of the process(s) and data being tested. All test scripts will be approved DHHS project team prior to their execution.
- User acceptance testing sign-off: User acceptance testing evaluation and sign-off will be the sole responsibility of DHHS.

PROJECT CONTROL DOCUMENTS (1.4)

Within two (2) weeks from the contract start date, the contractor shall submit plans for the project, including

VisualVault has read this requirement and will comply.

RISK MANAGEMENT AND RESOLUTION PLAN (1.4)

This provides a description of the tasks and activities that will be performed as part of the contractor's Risk Management Plan At a minimum it shall include the following:

Preliminary Risk Assessment
A description of the most significant project risks and a description of proposed mitigation strategies for each risk This assessment also includes a description of the impact associated with any identified potential failures
Ongoing Risk Identification Plan
A description of the contractor's ongoing approach to the identification of potential risks, tracking of potential risks, and provision of information to DHHS that supports the monitoring of risk across the project
Risk Response Plan
A description of the contractor's ongoing approach to the determination of actions necessary to reduce threats and enhance the Project's activities Where applicable, contingency plans for various risks should be documented and contingency plan triggers should be identified

Preliminary Risk Assessment

Our team will develop a risk management plan to verify that risks are identified, planned for, analyzed, communicated, and acted upon effectively. The plan will include how risks will be anticipated, mitigation strategies that will be considered, and the details of what information is included in the risk register.

We have identified the following potential risks to this project:

- Customer cannot fully communicate the details of the system or have a clear vision of optimal interaction with the system.
- Project staff turnover.
- Subject Matter experts are not available to answer questions or provide direction.
- Data provided for migration testing is unusable or cannot be mapped adequately to the new solution.
- Integration requirements are unknown.
- Lack of commitment by the customers team to understand the new solution.
- Vendors inability to communicate clearly what the solution will be for the customer.
- Vendors misunderstanding of requirements.
- Scope creep and changing requirements.
- Testing resources are available by the Customer and Vendor.

To mitigate the risks of the above items, there are various actions that need to be applied to a project. We first use the discovery sessions, specifications document development and acceptance as a tool to ensure a higher degree of knowledge transfer and understanding has occurred. During the development of the discovery sessions, the VisualVault team will work with the customer to acquire artifacts that represent input, processing and output of each process. The VisualVault team will communicate what they heard, what this means to the solution and make suggestions on how the system will work. Then the information is transformed into a specifications document. This document confirms how the system should work in its entirety. As the VisualVault team has questions about the specifications document, additional discovery sessions will be held to resolve those questions. As the specifications document is delivered to the customer, they have the opportunity to understand the proposed solution, visualize screen prototypes, review workflow diagrams and make corrections to how the system should work. The iterative development of the specifications document aligns the customer and VisualVault team to what the solution should be.

Ongoing Risk Identification Plan

VisualVault uses project management techniques to mitigate and resolve issues along the way. These techniques include project schedule management, communication plans, risk logs, issue logs and quality assurance plans. Additionally, as we work with your team, we will identify challenges and suggest solutions that we have identified in other projects.

All team members are encouraged to proactively identify and report issues. Issues are centrally logged and tracked to verify successful resolution. Issues are discussed during project status meetings and options for resolution are clearly presented for management consideration. Issues are tracked with dates needed for resolution to ensure the project remains on schedule.

Change Requests are part of the process to make course corrections along the way. Each change request will be analyzed to identify impact to scope, cost and time. Working together, VisualVault and the customer will determine if and when each change request should be included in the solution.

Risk Response Plan

Issues are proactively identified and tracked over the course of the project. All issues, requests, and decisions are centrally logged and discussed during project status meetings. They are included in the periodic status reporting. All team members and stakeholders are encouraged to identify issues and each one is addressed. VisualVault will proactively recommend alternatives, solutions, and mitigation plans for each issue. Issues are categorized by type and level of impact, and each issue is assigned to an owner. Each issue is assigned a date by which resolution is needed to keep the project on schedule. Issues are discussed with key stakeholders and client project management to approve the plan for resolution. The action plans are documented and circulated with designated team members to keep all interested parties informed. Timely resolution of issues is essential to keeping the project on schedule.

ISSUE MANAGEMENT AND RESOLUTION PLAN (1.4)

The plan presents a description of the contractor's standard process for resolution of problems identified and reported by the contractor and DHHS staff. This description must include the contractor's plan for ensuring that issues, requests, and decisions are recognized, agreed upon, assigned to an owner, incorporated to an issue log, monitored, documented, and managed

ORGANIZATIONAL CHANGE MANAGEMENT PLAN (1.4)

VisualVault's experience with projects of this size and scope has led us to the conclusion that organizational change management is essential to project success. It provides the underlying framework for our entire approach. Data migration is particularly vulnerable to problems without understanding the impact of this technological change on the people, processes, and technologies used by DHHS and its stakeholders/partners. We understand that working closely with DHSS to develop an Organizational Change Management Plan that defines the organizational change activities that support the successful transition from current to future technologies and processes is an essential project deliverable. We have considerable experience with organizational change management in the public sector, including specifying roles and responsibilities, processes, and methods necessary for communicating and managing organizational change during technological change processes.

We also have learned that assessing organizational readiness is an essential precursor to understanding DHSS' capacity, desire, and motivation for this change. Components of the readiness assessment would include, but not be limited to:

- A comprehensive assessment of DHSS' capacity for, and tolerance of, change,
- A stakeholder analysis, and
- An assessment of the system's overall change capacity.

WORK MANAGEMENT PLAN (1.4)

This part of the plan is for ongoing management of the *Detailed* Project Work Plan. At a minimum, this includes information on frequency of updates, a description of how schedule-related issues will be addressed, and a strategy for integrating elements of the Work Plan with Issue Management, Status Reports, and other related project management deliverables

VisualVault has included this in the SOW Section.

CHANGE CONTROL DOCUMENTS (1.4)

Change Control Process
The contractor must work with DHHS to establish a change control process. Change control is the formal process for identifying changes that arise in the natural flow of the project (but do not impact scope, deliverables, or budget) and determining the disposition of the requested change or correction. The Change Control Process will span the entire project life cycle and incorporate a formal change request process, including formal DHHS review and approval

VisualVault has read the above and agrees to work with DHHS to establish a change control process that works best for this project. Please see Attachment K2 Change Control for our documented change management policies and procedures included at the end of this proposal.

CONTROL REQUEST:

Provide a clear description of what is included from each change request
Delineate impacts to the project's schedule
Require successful completion of testing before the implementation stages
Incorporate multiple levels of priority for change requests (e.g., critical, must- have, desired, etc.)
Support the Change Control Process by estimating impacts, investigating solutions, identifying alternatives, inputting appropriate information into the Project tracking tools, participating in the decision-making process, and implementing the agreed-upon solution

VisualVault has read the above and agrees to work with DHHS to establish a change control request process that works best for this project.

CHANGE CONTROL TRACKING SYSTEM

The contractor must provide a change control tracking system that provides the following minimum requirements:

The means to control and monitor change requests
A process for reporting the status of all change requests
The ability for DHHS to set and change priorities on individual change requests

A method for DHHS to determine the estimated or actual hours allocated to each deliverable/project and the personnel resources assigned to each task

A method to generate a complete data provided by DHHS for each deliverable/project

VisualVault has read and agrees to comply with this requirement.

STATUS REPORTING PLAN (1.5)

The protocol for submittal of Status Reports, including the format and media for submittal and the procedures for submittal. Key in condition for these reports includes: summary of recent accomplishments, identification of resolution plans, and documentation of critical issues and risks (from issue and risk management tools), activities planned for the next reporting period, and a summary of the project's progress according to the schedule, budget, and task list. Schedule monitoring will include identification of any project schedule variance that has occurred. The contractor shall submit a form of month-end Status Report in a format approved by DHHS.

VisualVault has read and agrees to comply with this requirement.

PROJECT AND STATUS MEETINGS PROTOCOL (1.5)

This is the protocol for project Status Meetings. Status Meetings will be scheduled every week. The contractor's project management team, DHHS's Project Lead, and other key staff will attend the Status Meetings. Meetings will follow a standard pre-set agenda jointly prepared by the contractor and the DHHS Project Lead. The meeting agenda will be distributed twenty-four (24) hours before the scheduled meeting. The agenda should be flexible to allow discussion of other issues or concerns. The contractor must create written meeting records, in an agreed format, for the DHHS Project Lead. All meeting records and related documents will be stored in electronic format within the Electronic Project Library (EPL) (to include an index of meeting records).

VisualVault has read and agrees to comply with this requirement.

ELECTRONIC PROJECT LIBRARY (EPL) (1.6)

The contractor is required to use SharePoint to serve as a foundation for documenting contractor's efforts on this project and also acts as a repository to retain, share, and track critical project information. The EPL will include both current and historical versions of the Detailed Project Work Plan as well as all other project documents. The EPL will be maintained and remain accessible to both DHHS and the contractor's project teams throughout the life of the contract including all renewals and extensions. All project staff will be given appropriate folder-level and file-level access and restrictions according to standards agreed upon between the contractor and DHHS. The contractor will provide a description of the security measures that will be put in place to ensure that only authorized personnel have access to the EPL. As appropriate, all materials in the EPL will be indexed for easy retrieval. Contractor's designated documents and files will be maintained as part of the EPL.

VisualVault has read and agrees to comply with this requirement.

SECURITY PLAN (1.7)

The bidder shall describe how the proposed System shall provide application controls to prevent unauthorized use, maintain system process controls, and log all transactions. In addition, the proposed System shall provide security to limit availability to application functionality, software screens, data records, data elements, and data element values where appropriate.

If the contractor hosts the solutions, the contractor shall develop a Security Plan and document the contractor's plan to prevent unauthorized use and disclosure of sensitive and confidential data. The Security Plan shall include administrative, physical and technical safeguards. The plan must also conform to State and federal laws and regulations. The State must initially approve the Security Plan, and will, from time to time, conduct audits of the Security Plan. The contractor will provide full cooperation during those audits.

VisualVault promotes the extent we take to provide data security. We have read and will comply with these requirements.

The Aging Information System platform was originally developed as a compliance tool for medical manufacturers. As such, the core design was focused on controls that monitored every access, action, and activity. Any access, action, or activity is automatically recorded in the change log. The recorded data can be used to populate dashboards in real-time and to populate reports. The security plan will incorporate the information below and more.

VisualVault provides security to deny availability to the AIS platform. Typically, we integrate with the state's network authentication.

- Integration with third party SSO solutions is a core VisualVault feature. Third party SSO solutions must be SAML 2.0 compliant
- Oracle Identity Manager, Ping Identity, OKTA, OneLogin, Active Directory Federation Services

(ADFS)

In addition to the DHHS's single sign on, VisualVault leverages AWS' cloud to provide industry best practices surrounding data security. Additionally, VisualVault uses a combination of symmetric and asymmetric encryption algorithms called "Envelope Encryption" along with a centralized Key Management Service (KMS) to encrypt data at rest. The algorithm used for symmetric encryption is the Advanced Encryption Standard (AES). The algorithm used for asymmetric encryption is RSA. The reality is if anyone were to gain unauthorized access, call the content is encrypted at rest and in transit to prevent exposing confidential data.

VisualVault's use a key management service (KMS) where each tenant may have their own master key which is managed by the KMS. Customer does not have access to their master key; master key is managed according to our key management policy.

Please see the following reports on the VisualVault platform and security and data security

Attachment A - GRM VisualVault 2016-Type 2 SOC 2 Final Report
Attachment B - GRM VisualVault 2016 - HIPAA-HITECH Security Assessment-Final Report
Attachment H - GRM VisualVault IT Security Standard (STD-0001)
Attachment P - GRM VisualVault Encryption and Key Management

Screen shots of Change Logs

PAPP-000047 Rev 9

Close

Application | Documents | Forms | Change Log | History | Revisions

Form ID	Revision	Modify Date	User ID
PAPP-000047	2	7/20/2016 9:59:56 AM	test1@test.com

Field Name	Previous Value	Current Value
Applicant ID		PAPP-000047
Application Type	Select Item	Nursing Home
Authorization Signature		test1@test.com 7/20/2016 10:04 AM
DataField197		True
Sec B Current Cert Held	Select	No
Sec B Entity Revenue Type	Select	Profit
Sec B Legal Entity Mail Address		2020 W. Capital Ave
Sec B Legal Entity Mail City		Baltimore
Sec B Legal Entity Mail State		Maryland
Sec B Legal Entity Mail Zip		21206

PAPP-000049 Rev 7

Close

Application | Documents | Forms | Change Log | History | Revisions

Form ID	Revision	Modify Date	User ID
PAPP-000049	2	7/20/2016 12:43:43 PM	

Field Name	Previous Value	Current Value
Admin Application Status	Waiting Submission	In Review
Applicant ID		PAPP-000049
Application Type	Select Item	Pediatric Clinic
Authorization Signature		test2@test.com 7/20/2016 12:48 PM
DataField197		True
Sec B Current Cert Held	Select	No
Sec B Entity Revenue Type	Select	Profit
Sec B Legal Entity Mail Address		02 Lincoln Way
Sec B Legal Entity Mail City		Baltimore
Sec B Legal Entity Mail State		Maryland
Sec B Legal Entity Mail Zip		26201
Sec B Legal Entity Type	Select	Sole Proprietor
Sec B Legal Entity Website		www.tofA.com
Sec B Mailing Address Status	Select	Same

1 Page size 15 7 items in 1 pages

The History tab shows a list of events that have occurred against the case. Included, who edited, completed a workflow task and viewed the record.

PAPP-000049 Rev 7

Close

Application | Documents | Forms | Change Log | History | Revisions

Search

Form Name	Rev	Action	User Name	Date
PAPP-000049	7	Form viewed	demo config	8/26/2016 2:30:31 PM
PAPP-000049	7	Created form data revision 7	demo config	8/19/2016 12:18:25 PM
PAPP-000049	6	Unlocked form data revision 6	demo config	8/17/2016 2:24:22 PM
PAPP-000049	6	Created form data revision 6	demo config	8/17/2016 2:22:47 PM
PAPP-000049	5	Unlocked form data revision 5	demo config	8/16/2016 2:27:16 PM
PAPP-000049	5	Form viewed	demo config	8/16/2016 10:22:28 AM
PAPP-000049	5	Created form data revision 5	demo config	7/28/2016 11:07:49 AM
PAPP-000049	3	Created form data revision 3	demo config	7/20/2016 12:53:08 PM
PAPP-000049	1	Created Form Data	demo config	7/20/2016 12:05:57 PM

BUSINESS CONTINUITY / DISASTER RECOVERY (1.8)

The contractor must develop a Business Continuity Plan which includes the following:
Identification of the core business processes
For each core business process:
Identification of potential system failures for the process.
Risk analysis.
Impact analysis, and
Definition of minimum acceptable levels of outputs.
Documentation of contingency plans;
Definition of triggers for activating contingency plans;
Discussion of establishment of a business resumption team;
Maintenance of updated disaster recovery plans and procedures; and
Plan for replacement of personnel

VisualVault understands the responsibility to maintain a reliable infrastructure and environment. Towards that objective, VisualVault provides detailed documentation surrounding Business Continuity/disaster Recovery and associated plans that illustrate our focus on this important requirement.

Please see the following attachments included at the end of this proposal:

- Attachment F - GRM VisualVault Disaster Recover and Business Continuity Plan (ISO-0015)
- Attachment L - GRM VisualVault data Retention Backup and Restore (SPO-009)
- Attachment Q - GRM VisualVault Information Security Incident Management (ISO-0039)
- Attachment R - GRM VisualVault Information Security Incident Response Plan (ISO-0040 redacted)

PROPOSED DEVELOPMENT APPROACH

REQUIREMENTS ANALYSIS (2.0)

The outcome of Requirements Analysis is a set of documents that outlined the details of the system functionality. These documents will be developed in conjunction with the Functional and Technical Requirements Traceability Matrices.

REQUIREMENTS VALIDATION DOCUMENT (RVD) (2.1)

Attachments B and D contain DHHS' functional and technical requirements for the proposed solution. The bidder shall validate existing RFP requirements to provide the level of detail necessary for any further design, development, or implementation activities that address each of the two Divisions' requirements. Such further detail and definition are to be considered within the scope of the original RFP requirements and contract.

VisualVault has complied with this requirement. Please see Attachments B and D.

FIT/GAP ANALYSIS (2.2)

The fit/gap analysis will document the disposition of each requirement and the resolution of identified gaps (e.g., customization, workaround, alternate requirement). The contractor shall assist DHHS in identifying appropriate business process improvement opportunities, documenting the recommended changes, and planning and implementing approved business process changes. Traceability and mapping are key components throughout this process.

The VisualVault Team will work with DHHS during the discovery phase. That is also the time where our SME Mark Ervin former CIO of FL Department of Persons with Disabilities will provide insight from the system modernization project he oversaw at the Department.

PILOT/PROTOTYPE (2.3)

The Requirements Analysis activity will include a pilot prototype system integrated with the business process analysis and software configuration process.

VisualVault has read and will comply with this.

DESIGN, DEVELOPMENT, AND IMPLEMENTATION PHASE

The following table contains a list of the requirements and due dates expected of the contractor for the Design, Development, and Implementation (DDI) phase of the project. Details for these requirements follow, in the text after the table.

	Phase	Requirements	Please Insert Anticipated Timeframe
3.1	3.0 Design	Detailed System Design Document (DSDD)	Due dates to be determined in the Detailed Work Plan
3.2		Testing Plan	Due dates to be determined in the Detailed Work Plan
4.1	4.0 Development, Interfaces, Integration	Software Development Plan (if needed)	Due dates to be determined in the Detailed Work Plan
4.2		Development/Customization (if needed)	Due dates to be determined in the Detailed Work Plan

4.3		Software Development Summary Report(s) (if needed)	Due dates to be determined in the Detailed Work Plan
4.4		Schedule of interface development efforts	Due dates to be determined in the Detailed Work Plan
4.5		Interface Environment Setup	Due dates to be determined in the Detailed Work Plan
4.6		Interface Development and Testing	Due dates to be determined in the Detailed Work Plan
5.1	5.0 Data Conversion	Data Conversion Plan and Guide	Due dates to be determined in the Detailed Work Plan
5.2		Conversion Results Report	Due dates to be determined in the Detailed Work Plan
6.1	6.0 Testing	User Acceptance Testing Plan	Due dates to be determined in the Detailed Work Plan
6.2		System Testing Results Report	Due dates to be determined in the Detailed Work Plan
7.1	7.0 Training	Training Plan	Due dates to be determined in the Detailed Work Plan
7.2		Onsite Train-the-Trainer session(s)	Due dates to be determined in the Detailed Work Plan
7.3		Video sessions	Due dates to be determined in the Detailed Work Plan
7.4		Training Manuals	Due dates to be determined in the Detailed Work Plan
8.1	8.0 Implementation	System Implementation Plan	Due dates to be determined in the Detailed Work Plan

Remainder of page intentionally left blank.

	Phase	Requirements	Please Insert Anticipated Timeframe
8.2		Problem Resolution Plan	Due dates to be determined in the Detailed Work Plan
8.3		Final Readiness Assessment	Due dates to be determined in the Detailed Work Plan
8.4		Documentation	Due dates to be determined in the Detailed Work Plan
8.5		System Go-Live	Due dates to be determined in the Detailed Work Plan

Remainder of page intentionally left blank.

DESIGN (3.0)

As necessary to meet the requirements of this contract, the contractor will conduct design sessions, Joint Application Development (JAD) sessions, business rules sessions, and workflow sessions to develop the Design requirements. Prior to each session, the contractor shall develop/update proposed preliminary designs to the extent that it is possible and present it at the session.
The contractor shall evaluate the detailed design and test requirements considering:
Traceability to the requirements of the software item
Consistency with architecture
Feasibility of testing
Feasibility of operation and maintenance
Detailed System Design Document (DSDD) (3.1)
The DSDD shall be approved by DHHS. The DSDD must be updated to reflect changes identified through the DDI phase. Updated sections must be provided to DHHS for review and written approval within ten (10) days of a system change.

VisualVault will provide the information listed in this requirement.

The VisualVault Team's hybrid waterfall/Agile implementation methodology is designed to enable our team to perform a series of JAD/discovery sessions to gather requirements and prepare our Specifications Document. The Specification Document lists each functionality that is to be delivered. Graphics and other tools are included to allow DHHS staff to visualize and approve each. When the entire document has been reviewed, changes and been accepted, both teams sign the document and the final SOW may also be revised to align with the Specification Document.

DHHS will have ample time to continually review the specification document and make changes to assure it represents the solution you intend to use.

TESTING PLAN (3.2)

The contractor shall also define and document test requirements and a schedule for testing software units. Testing requirements shall include any compliance testing with the industry standards and regulations.

VisualVault agrees to document test requirements and provide a schedule for testing units.

DEVELOPMENT, INTERFACES, AND INTEGRATION (4.0)

DEVELOPMENT

Software Development Plan (4.1)
If needed, the contractor shall create the Software Development Plan which is an assessment of the contractor's methods and process for using a systematic, documented approach for all software development activities and the environment.

VisualVault is pleased to provide Attachment J - GRM VisualVault Software Development Life Cycle (SOP-006) included at the end of this proposal.

This document defines the concepts and requirements for the life cycle for software development at VisualVault. Following the software development life cycle (SDLC) model is critical for achieving compliance with industry standards and is a prerequisite for computerized systems validation. This standard operating procedure (SOP) describes the life cycle model, and the processes, activities and tasks associated with the various stages of the model.

Should DHSS require additional Information, VisualVault will be pleased to provide additional information upon request.

DEVELOPMENT/CUSTOMIZATION (4.2)

[illegible] the contractor shall complete any customization development.
. isualVault agrees to configure and customize all functionality agreed to in the Specification Document that is the basis for all functionality to be created for the AIS platform.

SOFTWARE DEVELOPMENT SUMMARY REPORT (4.3)

If needed, the contractor shall provide to DHHS a Software Development Summary Report (4.2) during the Development work as requested. The report must contain, at a minimum:
Major products developed, delivered, or updated
Identification of all issues that have arisen and resolutions (identification of issues/risks that may impact the next phase)

The VisualVault Team agrees to this requirement.
VisualVault is also pleased to confidentially share our product roadmap to allow DHHS to understand upcoming new functionality.

INTERFACES

Two AAAs use Mediware SAMS product. The proposed system must electronically interface client and service information with Mediware SAMS product.
The proposed system must interface at least four times per day.
The proposed System must also support functionality to extract a file in a standard file format (i.e. xls, cvs, etc). Appendix A-1 & 2 reflects software in production.
Schedule of interface development efforts (4.4) Develop a master schedule of interface development efforts (4.4) that is integrated with the Detailed Project Work Plan.

- VisualVault agrees with the need to provide a master schedule of interface development efforts once the JAD sessions have provided the details for each.
- VisualVault understands the electronically interface with the Mediware SAMS product.
- The AIS platform supports functionality to extract files in standard formats.

INTERFACE ENVIRONMENT SETUP (4.5)

The Contractor is responsible for ensuring that a stable and accessible interface testing environment is available by an agreed upon date

The VisualVault Team agrees to fulfill this requirement.

INTERFACE DEVELOPMENT AND TESTING (4.6)

The contractor shall be responsible for developing all the necessary interfaces. This includes interface design, development, validation, testing, and documentation. DHHS will coordinate any required interactions with other parties who will need to modify their systems to use these inbound and outbound interface datasets.

The contractor shall be responsible for developing interface standards for any electronic interfaces into the proposed System. The contractor shall also assist the electronic interfaces into the proposed System by providing consulting support and assistance with testing at no additional cost to the State.

VisualVault has read and will provide the required interfaces. To expand on our capabilities, please see the following.

Integration is a strength of the VisualVault solution and is core functionality. VisualVault has read and agrees to these requirements as long as the 3rd party applications are open and integrate to other systems as a general practice.

A foundational piece of the VisualVault platform is our suite of Enterprise Content Management Services used to implement and support business process automation including high volume document and intelligent form-based processes. Core platform capability includes: Intelligent iForms, workflow, records retention, reporting, configurable user interface, micro services library, data connections library, and extensive APIs. System integration is achieved using the following VisualVault capabilities:

REST API - Platform & language neutral API which can be used to import data, submit electronic form records, upload files, attach or relate files and forms, create/edit users and groups, search forms and documents download files. The API could be used to auto reconcile agent records with an external system on a scheduled basis.

MICRO SERVICES LIBRARY - VisualVault micro services library supports Node.Js scripts or web service end point addresses. Node.Js scrips can interact with VisualVault APIs as well as other system's APIs including any of DHHS' other system which provide API accessibility. Node scripts can be developed and tested against the VisualVault APIs on a local computer with Internet access and then uploaded to VisualVault's micro services library for production use. Node.js scripts or Web service end points can be scheduled for automatic execution or can be used by VisualVault's intelligent forms to provide customer specific data validation, business process automation, and data import / export capability.

FORM / DOCUMENT IMPORT SERVICE - VisualVault provides an import service for flat files (csv) and attachments. Files can be sent using a pre-configured SFTP account which will auto-import files as they are received. The document import service is commonly used to intake documents from intelligent capture systems such as EPHESOFT, Kofax, or document production systems.

DATA CONNECTIONS LIBRARY - VisualVault provides a data connections library designed to allow direct data queries against Oracle or Microsoft SQL Server databases via Web Services. The data connections library is commonly used by iForms to populate form drop down lists, document index field drop down lists, or auto-populate form fields as a user is filling out a form. Additionally, the VisualVault API can access the data connections allowing a micro service to query data and use it for validation of business rules.

DATA CONVERSION (5.0)

The contractor shall have responsibility for converting client demographic data from the NAMIS and ADRC referral dashboard systems into the proposed System. The contractor will work with DHHS to obtain data conversion files containing the data elements in the format and the agreed-to timeframe necessary to support testing, conversion, and overall project plan.

Data conversion/migration is one of two areas that can quickly disrupt the project. Therefore, the VisualVault Team places a significant emphasis on this part of DHHS's project.

The VisualVault data conversion approach is based both on VisualVault's successful record of accomplishment as well as the expertise our teaming partner ProCom brings from large commercial and public-sector data migration in regulated environments where both the timing and accuracy of data migration is paramount. For example, since 1999 Frontier Communications has relied on ProCom to provide data migration to support post-merger integration and other major technology projects, with a total of more than 50 Billion data records and more than 1.5 Billion documents successfully migrated from multiple source systems.

We understand and agree with your requirements and key goals for data conversion, and specifically:

- It is our practice to develop and get joint agreement on a data conversion plan that documents the approach and timing of conversion activities; special constraints and known issues regarding the source data, stakeholder groups and subject matter experts that need to be engaged; approach for control and validation to support go/no-go decisions; recovery and backup plans; and the business impact on operations. Key principles for the data conversion plan will be that all source data records will be accounted for and that the cutover to production is carefully planned with the focus on controlling the impact to operations.

- Our data conversion and migration methodology is designed to minimize impact on operations by careful planning to keep down time during the migration to production to a minimum. We achieve this by executing multiple (a minimum of three) mock conversion test runs which allows us to find issues and refine the data conversion as well as confirm timing and processes/checklists to successfully complete the migration activities as well as streamline the processes to keep the conversion window as short as possible. During our conversion planning we also work with your team to understand business impact such as avoiding peaks of high workload for system downtime, conducting the data migration during non-working hours (ex. over a weekend), identifying data that can be migrated to a "sandbox" environment and validated early (ex. historical transactions) in order to streamline the timing for production migration, accounting for any natural business processing cutoffs, and considerations of the merits of a single migration versus incremental/phased cutover.

- In coordination with your technical team, we develop a backup and recovery strategy during the data conversion planning and test this strategy during the multiple mock conversion test runs.

- We recognize the importance of maintaining data integrity to comply with annual Federal reporting guidelines. Our expertise has been developed through the successful data migration of billions of records in regulated industries where data integrity is necessary to follow regulations. We develop detailed control reports that account for every source data record and are designed to support your staff in validation and go/no-go decisions. We use multiple test runs to refine the extract, transform, load process and the control reports to support this goal.

The following describes the process for data conversion. We have assumed that data dictionaries are available, and that data cleansing is limited to resolution of the issues identified in your answers to questions that some records will have missing information in required fields and some system codes will not be available when migrating to the new system, as discussed below.

1. **Data Conversion Planning** - during this activity, we will work with your team to develop a comprehensive data conversion plan that will serve as a roadmap and will take into consideration not only the technical migration, but also impact on operations associated with migration activities, such as potential impact on legacy system availability during the data conversion process. We understand and affirm that important goals include minimal impact to

the Department's operations, that down time is to be kept at a minimum, and that a recovery and backup method will be included with the data conversion plan. During this activity, we will also work with your technical staff to determine the tools and methods for data conversion, including the following options:

1. Establish a connection to the data source, typically using the VisualVault Data Web Services application which can be installed on your server. This approach allows your staff members to define data connections and queries to SQL Server or Oracle databases which provide VisualVault with read-only access.
2. Export the seed data to flat files and send via FTPS for bulk import
3. Jointly agree upon a custom data interface connecter using web services and/or third-party Extract, Transform, Load (ETL) tools. We have experience with a number of ETL tools, including the Talend open source tool, or we can work with ETL tools that you currently use if preferred.

2. **Data Mapping** - during this activity, our team, working with your IT staff and business users, will identify the legacy systems data source systems and map the data elements to the target data base. We will also identify data elements required by the new system that are not available in the legacy system and develop an approach for these data elements to be inserted in the seed data, which may include manual data entry either prior to or after data migration.

3. **Data Extraction and Transformation** - during this activity, we will define the data extraction processes. We will define the rules to validate data, required data transformation activities, and other data conversion activities required. We will then perform data extraction and transformation in a test environment, typically running the tests multiple times, providing your IT and business users the opportunity to validate the extraction process success, including the converted data maintaining data integrity to comply with annual Federal reporting guidelines. As indicated in your answers to questions, it is our understanding that there is a known issue where the source system (the Early Steps Administration System-ESAS) includes some records with missing information in required fields and that some systems codes will not be available. The primary objective is to migrate data through automated routines, and only where business rules cannot be identified to support automated data transformation or where necessary data elements are not available, will the source data be migrated "as is" to the target database, potentially requiring subsequent data correction (see activity 7 below). We will work with your team to define business rules and develop automated scripts for the transformation required to achieve this objective.

4. **Control Report Development** - during this activity, we will develop reports that measure data as it flows from the source system to the target system with the overall objective that every record can be accounted for. Measures typically will include number of accounts and other key metrics unique to the source and target systems. We will also include measures to demonstrate the data integrity to support compliance with annual Federal reporting guidelines. We will work with you to develop reports that will allow both functional and technical decision makers to validate that data has been successfully migrated to support go/no-go decisions. We can use the Jaspersoft open source reporting system or reporting tools you currently use, if preferred.

5. **Mock Data Conversion Iterations** - we will conduct several mock conversions of data and where possible provide converted data as input to the testing processes to receive feedback and continuously improve the data conversion accuracy and completeness. Your IT staff and business users will be able to include live converted data in the user acceptance test phase of the implementation. The import to the integration test may not include the full data set or a subset that is representative of the full data set and sufficient to support the user acceptance test. As a result, we will have executed multiple "mock migrations" prior to the final migration to production. This iterative process is the best practice for data migration, since data issues are often not identified in the initial run, and each additional run improves the accuracy and completeness of the process.

6. **Data Migration to Production** - Following the conclusion of user acceptance test, we will make any required updates to the data extraction, conversion, and import routines, and run one or more migration tests with the full data set, producing audit control totals to validate that the full data set has been properly imported in a test environment before running the final data migration into the production environment. We will provide final audit control totals and other migration results reporting to allow your IT and business users to validate the successful data migration into production.

7. **Additional Data Corrections (OPTIONAL)** - During any of the prior data conversion activities we may identify data that will require corrections, but where automated transformation cannot be performed for any of several reasons, typically due to missing data in the source systems or inability to define business rules that can be uniformly applied. In these situations, we will migrate the data "as is" and provide options and estimated effort for subsequent data correction activities.

ATA CONVERSION PLAN AND GUIDE (5.1)

The contractor shall lead interactive conversion strategy sessions with DHHS and other stakeholders to develop a Data Conversion Plan that addresses all components of the data conversion phases to include but not be limited to. development of conversion rules and process (Conversation Guide (5 2)) such as data element mapping crosswalks, data cleansing, data synchronization for initial and interim conversion activities leading up to the final data conversion, and frequency of interim conversion events and final conversion execution

The VisualVault Team will comply with this requirement to provide the transparency DHHS requires. Please see a portion of the detail we plan to provide in the previous answer.

CONVERSION RESULTS REPORT (5.2)

The contractor shall execute the data conversion activities according to the Data Conversion Plan and Guide The final step of the data conversion process is the Conversion Results Report

The VisualVault Team will comply with this requirement to provide the transparency DHHS requires. Please see a portion of the detail we plan to provide in the previous answer.

TESTING (6.0)

The contractor shall be responsible for conducting unit, system, and integration testing for all programs, modules, and sub-systems throughout the development and management life cycles. The contractor is responsible for successfully completing system and user acceptance testing prior to implementation.

The contractor is responsible for certifying that each program, module, and sub-system meets or exceeds all of the functional, technical, and performance requirements prior to implementation. The contractor shall be responsible for working with DHHS to establish testing environments that mirror the production environment.

VisualVault agrees we are responsible for unit, system, and integration testing throughout the development and management life cycles. We are responsible for successfully completing system and user acceptance testing prior to implementation. NE DHHS is responsible for approving the tests by using the test scripts provided by The VisualVault Team in an agreed to timeframe. Sign off is required by DHHS after completing the test cycle if a positive test is completed.

User Acceptance Testing is conducted upon the conclusion of each Sprint and again upon completion of all Sprints or completion of a Program Increment (group of Sprints).

USER ACCEPTANCE TESTING PLAN (6.1)

The contractor is also responsible for the initial development of User Acceptance Testing test scenarios, building detailed testing scripts, determining expected results, establishing testing procedures and protocols, etc. DHHS must approve in writing all test scenarios prior to testing. Acceptance testing will include testing by users of all system functions, including but not limited to, proper functioning of software, hardware and network components as well as both data content, output, and connectivity components. It also offers the opportunity to test documentation, procedures, and business processes.

VisualVault is aligned with DHHS' Best-Practice method the User Acceptance Testing. Roles and responsibilities will be clearly delineated by VisualVault and agreed to by DHHS.

USER ACCEPTANCE TESTING RESULTS (6.2)

The contractor is responsible for the management of the testing effort and other related events and communicating this ongoing information with the State testing team. The contractor must provide DHHS with all test results, to include the tracking and correction of deficiencies. DHHS will not procure testing tools for this project and any testing tools proposed shall be provided by the contractor and licensed by the contractor for use by its staff and the applicable DHHS staff for the project at the testing site. If needed, the contractor shall provide any required training on the proposed testing tools to all State staff that will be required to use the proposed testing tools at no cost to the State. At the end of the engagement, testing artifacts will be transferred to DHHS. The contractor shall also provide any needed testing infrastructure (desktops, servers, etc.) and/or licensing to support any contractor-provided testing tools.

VisualVault affirms that a test plan will be maintained and provided to DHHS. Training will be provided on the test plan to assist the State testing team in conducting and validating test results. A list of issues encountered during testing will be maintained and prioritized for resolution. VisualVault affirms that the State does not need to acquire testing tools and that all artifacts representing the testing will be provided to DHHS at the close of the project. A testing/sandbox site will be provided for conducting all testing during configuration of the system and for testing bugs after the system goes into production.

TRAINING (7.0)

Introduction--VisualVault's Approach to Training.

VisualVault's approach to Training is based on our Organizational Change Management Framework–a systems approach with five component-parts--communication, organizational readiness, training, knowledge transfer, and user support. These five components are interrelated and interdependent and the system itself is dynamic and changing. A change in one component of the system affects other components. As the graphic below demonstrates, all of the interrelated, interdependent components are necessary to build SUA capacity to operate and "own" the *AIS* solution.

The success of our work with SUA to develop and deliver Training will depend on the extent to which we accommodate existing *communication* patterns and, possibly encourage new patterns. Our ability to successfully *transfer knowledge* to SUA staff will be highly dependent on the effectiveness of our Training delivery and our continuous learning approach. Organizational *readiness assessments* not only assess SUA staff motivation, desire, and capacity for change–they identify important training approaches, delivery methods, and content/curricula. How we assist with *user support* activities is interrelated with communication patterns and channels, post-implementation activities such as transferring knowledge and transitioning to SUA "ownership" of the Solution, and SUA's overall readiness for and capacity for the technological change.

It follows, then, that our Training approach is along the same holistic "systems" path as our OCM Framework–we approach all training efforts based on four interrelated, interdependent components. This methodology, which is based on best practices and proven experience, is clear and well-defined to minimize risk and enhance communications of risk ms and action plans, includes planning, development, delivery, and evaluation.

TRAINING PLAN (7.1)

The contractor shall detail all activities for training in the proper use of the proposed System. It will provide a description of the train-the-trainer strategy including methods, materials, and timing. The contractor must submit the Training Plan to DHHS two (2) months prior to the train-the- trainer session(s). This will allow time to prepare the necessary logistics for the session(s).

Our planning will include configuration specifically for Nebraska's SUA Aging Information System Software needs, including Nebraska Aging Management Information System (NAMIS) replacement, case management and services (Mediware@, SAMS), and an information and referral database. client services, care and case management, funding splits, administration requirements, and federal reporting requirements.

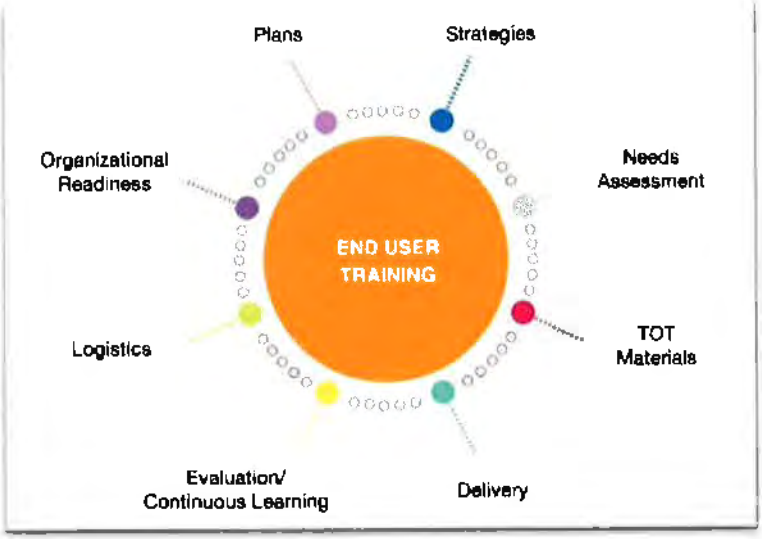
Our planning efforts will be guided by a Training Plan which will define required training, define the process for delivering the training, & define the stakeholders who will receive the training. We recommend that Nebraska SUA's Training Plan also incorporate Knowledge Transfer activities–those that define the process for transferring system and technical knowledge/information to the appropriate staff.

The Training Plan will specify tasks, methods, materials, and timelines regarding use of our Solution in the following areas:

- Initial understanding, navigation, and use for all *involved in the defined processes*
- Initial understanding, navigation, for *"train the trainer"* team members
- Initial understanding, navigation of the system for *SUA staff*
- Initial understanding, navigation of the system for e*xternal stakeholder/partner users*
- Initial understanding, navigation of the system for System Administrators (SAs)
- Master VisualVault use for all, including SAs
- Leadership training to familiarize each on navigation, use, with a keen focus on reports and how to use them to improve performance and how to track service improvement
- Use of dashboard and reports to document the expected 15% up to 25% reduction in staff labor hours dedicated to NAMI documentation activities.

The Training Plan will provide the necessary structure and processes for SUA and its stakeholders/partners to develop the knowledge, skills, and abilities necessary to operate our Solution. We recommend submission of a Training Completion and Knowledge Transfer Acknowledgement Report to confirm delivery and completion of transition to SUA operation.

DEVELOPMENT



VisualVault's training is designed for the different user groups who have varying education requirements based on system use. We develop our training to maximize the user experience by gaining the knowledge required to transform their workday. We develop training strategies that seek to enhance the student's learning experience by incorporating active learning techniques and leveraging SUA Subject Matter Experts (SMEs). This methodology, which is based on best practices and proven experience, is clear and well-defined to minimize risk and enhance communications of risk items and action plans.

Our training is based on adult learning principles and inclusive of a variety of learning styles. We develop training based on some assumptions about how adults learn (Malcolm S. Knowles):

- Adults want to know why they should learn.
- Adults need to take responsibility.
- Adults bring experience to learning.
- Adults are ready to learn when the need arises.
- Adults are task-oriented.

And adults have different learning styles–visual, auditory, and experiential/kinesthetic. Research confirms that we retain approximately 10% of what we see (visual), 30-40% of what we see and hear (visual and auditory), and 90% of what we see, hear, and do (visual, auditory, and experiential). Our proposed training methods address these issues and include readings, videos/slides, lectures, group discussions, examples, role plays, and practice demonstrations–all three learning styles. Our training types have included on-site classroom curriculum, instructor-led, self-paced and self-study, web-based live and recorded sessions for "external" community users (which we have found to be particularly effective for providers), mobile functionality & use of iForms off-line for field inspectors and investigators, and onsite or remote refresher training. We are accustomed to conducting training on policy and/or business process changes, application builds or releases, special or infrequent procedural updates, gap identification and remediation, and training for leadership on navigation and report use. Materials and manuals (Section 7.4 SOW) to support our training efforts can be customized based on SUA needs and can be provided via web portal, CD, or other appropriate method. Training manuals including an online Quick Reference Guide will be provided documenting the use of the VisualVault solution. This manual will be used in conjunction with the Solutions Training classes listed below. This manual will serve as documentation for how the solution operates at the time it is implemented.

Thus, we use a wide variety of training methods:

- On-site classroom curriculum
- Instructor-led
- Self-Paced and Self-Study
- Web based live and recorded sessions for "external community users such as Providers
- Particularly effective for provider education
- A portion of the training is designed for field inspectors and investigators to use VisualVault mobile functionality and how to use iForms off-line
- Refresher training can be scheduled and performed onsite or remotely
- Policy and/or Business Process changes
- Application Builds or Releases
- Special or Infrequent procedural updates
- Gap identification and remediation.

- We customize our training to fit the needs of our customers. Our experience has led us to categorize our training based on the following target audience:
- Mandatory - contractually required for assignment to the project [i.e. HIPAA, Security, Fraud, Waste and Abuse, Rights and Responsibilities, etc.]
- Functional Role/Job Specific - to perform a job or function [i.e. system navigation, processing of various submitted materials, complaint reviews, case tracking, etc.
- Supervisory or Lead - team operations and management
- System Administrative - Learning how to navigate, resolve minor issues, make changes to iForms, workflows, etc.
- Leadership - Educate management on navigation and report use.

TRAIN-THE-TRAINER SESSION(S) (7.2)

The contractor shall provide onsite training (6.2) for approximately twelve (12) trainers at a single DHHS location in Lincoln, Nebraska. Training materials for the train-the-trainer session shall be provided to DHHS a minimum of three (3) weeks before the onsite training session(s). The contractor shall provide leave-behind materials specific to the trainer group and will be available for limited on-going advice to ensure the success of the train-the-trainer approach.

The contractor shall provide, at no additional cost to the State, supplemental training for the trainer group if the State determines that significant system updates occurred. This supplemental training may occur onsite or via video conference, web portal, manual, or other mutually agreeable delivery method.

DELIVERY – WHAT KNOWELDGE ARE WE CONVEYING DURING TRAINING?

Delivery can include a variety of formats, taking advantage of best practices, experience and latest technologies. Our training is performance-based to ensure that SUA staff, Providers, and other community users can perform their tasks/work more efficiently.

We rely heavily on Train-the-Trainer strategy (Section 7.2 SOW) to ensure that SUA develops capacity to operate the system as quickly as possible. All training classes will include a combination of lecture, discussion, question and answer as well as hands on practice. Using these mechanisms, users will come to know the functionality, understand the technology supporting the functionality, and have a channel to ask questions and resolve challenges. We will provide onsite training for approximately twelve trainers at a single DHHS location in Lincoln, Nebraska. We will provide training materials to DHHS for the train-the-trainer session three weeks before the onsite training session(s). We will leave-behind materials specific to the trainer group and will be available for limited on-going advice to ensure the success of the train-the-trainer approach.

We will provide supplemental training as needed--either onsite or via video conference, web portal, manual, or other mutually agreeable delivery method.

The knowledge we convey during our training includes the following (by target audience):

- Training for System Administrators - These classes are preferably conducted on site and are designed for the individual or team that will be administering VisualVault. This training covers all aspects of managing VisualVault and provides attendees the tools to administer, identify issues, configure and train other individuals on the use of the product. The duration of this class is 5 days.

- Train-the-Trainers Training - This class is focused on the use of the solution. The focus of this training is to train staff trainers. These classes are much shorter in duration and focus on teaching the trainers all aspects of using VisualVault. These individuals will be able to train and teach others how to use the implemented solution. It is preferred that a core team of people be trained in person. Others can be trained via web meetings as well.

- Field Staff Training - These classes typically are conducted remotely using a "WebEx" type tool and will be for staff community users that cannot join the classroom events. This training will cover all aspects of managing and using VisualVault and will give the attendees the tools they require to use all aspects of the system.

- Leadership Training - This class will focus on the department leaders who are responsible for the management and oversight of the organization. This is meant to be a small group to allow individual's the environment to ask questions on a topic that is unfamiliar to them. The goal of this training is to have the leadership team use the system for the limited tasks required as well as gain a full understanding of the reporting capabilities and how to search, find, open and use their individual dashboards and reports to leverage the vast amount of performance data that will now be at their fingertips.

We have found that, approximately 60-90 days after Go-Live date, refresher training is important. This allows users to ask questions based on practical experience with the Solution. We will make video training available for these sessions (Section 7.3 SOW). Multiple instances of each function will be developed if necessary. These video sessions will be provided via web portal, CD, or other mutually agreeable delivery method.

How VisualVault's Approach to Training Guarantees Success– Evaluation and Continuous Improvement

VisualVault Training Staff regularly participate in continuous improvement (CI) efforts on all projects, including quality management processes, as well as *internal* CI processes. The purpose is to identify potential gaps in existing processes and to provide solutions for filling the gaps.

The VisualVault quality management process uses formal and in-formal audits and observations, operational observations and data, and QA / QC formal assessment data to identify gaps and problems in individual and collective performance in the operational areas. The issue may be found either in the training delivery or development, or both. VisualVault examines a variety of inputs, including output metrics, observations and information from our operational performance to determine those areas that need improvements. Our Training Staff develop the solutions appropriate for the given root cause - with the goal being identification of areas for improvement, and the creation of solutions and corresponding training that address identified weaknesses or improvement areas.

We use frequent in-class assessments and evaluations to understand how well the curriculum is being retained and determine what portions need to be repeated to assure a high retention level. The immediate feedback allows the instructor or mentor to apply additional training to remedy the identified student learning shortfalls. VisualVault expects ratings of 90% or greater on training evaluations.

VIDEO TRAINING MATERIALS (7.3)

The contractor shall make available video training for those who need a refresher lesson after the training. Multiple instances of each function will need to be developed if there are variations between the participating AAA's as each may have a slightly different view of the system (menus, options, and workflow differ based on user log in). These video sessions may be provided via web portal, CD, or other mutually agreeable delivery method.

VisualVault records training sessions as a best-practice and will do so for the NE project.

TRAINING MANUALS (7.4)

The contractor shall provide manuals for each type of training (such as new user and administrator) including quick start guides and FAQs. These manuals may be provided via web portal, CD, or other mutually agreeable delivery method.

VisualVault always provides training manuals for each client. The VisualVault Team will work with NE's DHHS team to present manual outlines to allow you to provide input to what works best for your team and the community of users.

SCREEN SHOTS OF TRAINING MANUAL

Please see next page.

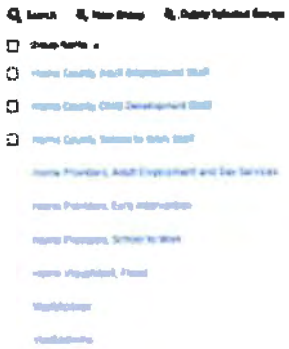
Remainder of page intentionally left blank.

6 Administrator Help

6.1 Orientation to Security Groups

The following depicts the groups which are setup in Visual Vault. These groups will define the Security that each user in the group will have.

Group Administration



6.2 Creating a New County User

The above image depicts Active Directory groups that are used. To create new county users, each user will need to be added to the Active Directory Group which matches the VisualVault security level. This will be propagated into VisualVault. Verification of the propagation may be completed by looking at the User Admin and Groups Admin areas.

6.3 Changing Data Using Admin Override

As an administrator in VisualVault, on the bottom of many of the screens, there is a checkbox for Admin Override. Many times there are read only fields throughout the form to lock down and secure fields that are changed by the system. There are also hidden fields that are used for similar purposes. When this box is checked, administrators will be able to see all of the fields and manually change read only fields.

- If this box is left checked, other users will have edit access to the fields as well.
- Administrators should refer to the specifications document to make appropriate changes to data when they choose to manually edit read only fields.

What Does This Mean for The Nebraska DHHS AIS System & Program?

1. *Training Excellence is Core to VisualVault*
2. *Change Management is not a risk issue with the inclusion of Stephenie Colston team partner SME*
3. *Superior documentation*
4. *Rapid acceptance rate based on VisualVault's approach*

IMPLEMENTATION (8.0)

NE DHHS will be working directly with the software company and our national implementation partner ProCom Consulting. The combination gives you direct access and proven team.

SYSTEM IMPLEMENTATION PLAN (8.1)

The Contractor shall develop a System Implementation Plan that includes, but not limited to:
Activities needed, milestones, prior to implementation
Staffing requirements
Communication activities
Plan for completion of knowledge transfer
Checklists of work to be performed and/or outputs to be produced on the first day and at the end of the first week, month, quarter, and year of operation
Rollback plan, which should include what will be done if the implementation does not succeed

VisualVault will provide this plan.

PROBLEM RESOLUTION PLAN (8.2)

The contractor shall establish procedures for receiving, recording, and tracking problem reports and modification requests from users and providing feedback to users. Whenever problems are encountered, the problems shall be recorded and entered into the problem resolution process.
The contractor and DHHS will develop a mutually agreeable Problem Analysis and Resolution Plan prior to completion of the system implementation.

VisualVault has our internal ticket application to manage problem resolution. We will develop the plan that aligns with your expectations with our Best-in-Class approach.

FINAL READINESS ASSESSMENT (8.3)

The contractor shall create the Final Readiness Assessment to assist in the determination of final implementation readiness. Written approval of this Assessment constitutes DHHS' decision to move forward with implementation. At a minimum, the Assessment must address the following:
An Assessment Summary that includes the analysis completed, risks, and mitigation associated with implementation and a recommendation for proceeding
Status of data migration/conversion efforts and its completion
An assurance that Disaster Recovery, where applicable, is documented and ready
Documentation of user acceptance testing approval by DHHS
Knowledge transfer sign-off by DHHS
Assurance that all locations, system users, and security profiles have been identified and set up
Documentation that Help Desk is ready and staffed for deployment
Confirmation that training participants designated in 7.2 (Onsite Train-the-Trainer session(s)) are available and ready to assist at a central location to be determined at a later date for initial deployment
Throughout the DDI Phase, the contractor's objective shall be to implement all required system functionality. The proposed System shall satisfy contractual functional and technical requirements, and conform to the approved System Implementation Plan.

VisualVault also understands the importance of a Final Readiness Assessment to assist in the determination of final implementation readiness. We would recommend that, in addition to the following information, the elements from the initial readiness assessment be included to articulate the impact of organizational culture on an organization's ability to effectively transfer knowledge from this project to DHSS' long-term sustainability of the Solution.

We will ensure the Final Readiness Assessment includes the following:

1. An Assessment Summary that includes the analysis completed, risks, and mitigation associated with implementation & a recommendation for proceeding;
2. Status of data migration/conversion efforts & its completion;
3. An assurance that Disaster Recovery, where applicable, is documented and ready;
4. Documentation of user acceptance testing & approval by DHSS;
   KT sign-off by DHSS;
5. Assurance that all locations, system users, & security profiles have been identified and set up;
6. Documentation that Help Desk is ready & staffed for deployment;
7. Confirmation that training participants designated in 7.2 (onsite train-the-trainer sessions) are available and ready to assist at a central location TBD at later date for initial deployment.

DOCUMENTATION (8.4)

Additionally, the contractor must develop and maintain the following documentation:
On-line Help (8.4) for all web portal features, functions, and data element fields, as well as descriptions and resolutions for error messages, using help features including indexing, searching, tool tips, and context-sensitive help topics.

An online, third party tool will be used to create and manage online help. This will then be integrated with each data entry screen so that users can find contextual documentation.

On-line User Manual (8.4) with a printable version available. The documentation should include full mock-ups of all screens/windows and provide narratives of the navigation features for each window/screen.

Online, third party tool will allow for the generation of printable documentation.

On-line Reporting Manual (8.4) with a printable version available that includes descriptions, definitions, and layouts for each standard report. Include definitions of all selection criteria parameters and each report item/data element, all field calculations defined in detail, and field and report titles.

Online, third party tool will allow for the documentation of these items and the generation of printable documentation.

On-line Installation and Technical System Operation Manual (8.4) with a printable version available. The documentation should include operating procedures to assist technical staff in operation and maintenance of the system. These procedures help define and provide understanding of system operations and performance. Documentation for all hardware and software products including reference guides, user guides, technical guides/manuals and technical documentation (e.g. system administration, configuration workbook, system architecture, application architecture, etc.)

As a content services platform product, VisualVault is installed in the VisualVault cloud environment. An installation manual is not needed. The customer will be provided a Technical System Operation Manual that communicates the features and capabilities of VisualVault. It will be provided in a printable format.

SYSTEM GO-LIVE (8.5)

System go-live is the date on which the solution has been fully implemented and meets all established functional and technical requirements. Based on Federal requirements DHHS's target implantation date is July 1, 2019 but will consider plans with a Go-Live date no later than October 1, 2019. The System Go-live date is dependent on DHHS's approval.

VisualVault has read this requirement and our implementation time line aligns with the required implementation time-frame. Please see our Implementation plan.

1. *Planning and documentation meets and exceeds all requirements*
2. *The VisualVault plan includes the number of resources at all positions to successfully deliver all documented functionality no later than October 1, 2019*

OPERATIONS & MAINTENANCE PHASE (9.0)

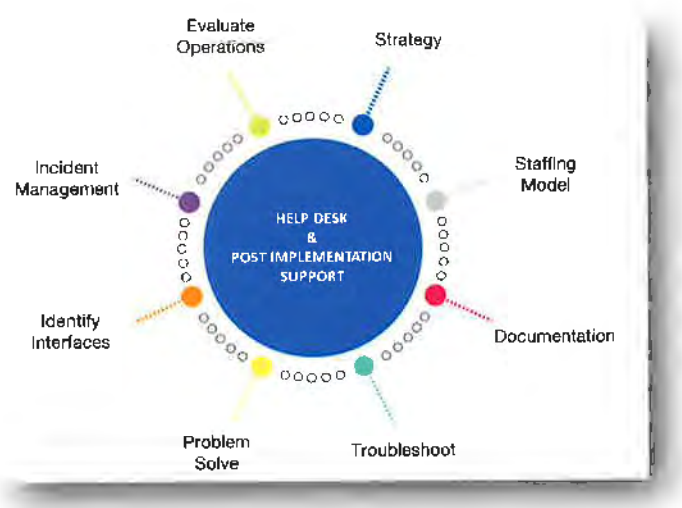
The following table contains the list of requirements and due dates expected of the contractor for the Operations and Maintenance (O&M) phase following the implementation of the solution. Unless otherwise specified, the requirements will follow in the narrative after the table.

	Phase	Requirements	Due Date
9.1	9.0 Operations and Maintenance	Operating Procedures Guide	Due dates to be determined in the Detailed Work Plan
9.2		Help Desk	Due dates to be determined in the Detailed Work Plan
9.3		Problem Resolution	Due dates to be determined in the Detailed Work Plan

Operations & Maintenance (O&M) activities include, but are not limited to: the following:

- Perform system maintenance, including testing, documentation, etc.
- Record, track, and resolve system defects at no additional cost to the State
- Maintain ongoing operations
- Conduct necessary software updates
- Conduct maintenance of interfaces
- Provide help desk support with predefined technical support prioritization levels
- Provide security management
- Support policy and process changes
- Keep portal up to date
- Keep all written material, including all system documentation and scripts, up to date as changes occur

VisualVault agrees to include all the above Operations & Maintenance activities as part of this proposal. It is assumed that "support policy and process changes" are specific to how the solution is supported by through the levels of issue reporting and does not equal reconfiguring the system outside of the scope of the specifications document.



OPERATING PROCEDURES GUIDE (9.1)

The contractor shall develop and maintain documentation on operating procedures to assist technical staff in operation and maintenance of the proposed System. These procedures help define and provide understanding of system operations and performance. The operations procedures will address all facets of the technical operation of the system. The Operating Procedure Guide must be continuously updated (at a minimum quarterly) to reflect the latest changes.

VisualVault will maintain documentation on operating procedures to assist in operations and maintenance of the proposed system.

HELP DESK (9.2)

The contractor shall be responsible to operate and support the Help Desk, and shall be responsible for providing a single toll-free number and a single local number for use. The contractor shall also provide voice mail capability and shall provide an on-call staff person with paging capability during non-operating hours.

The contractor shall create the Help Desk Procedures Manual, which defines and documents the processes and procedures for Help Desk operations. These procedures will include, at a minimum, problem identification and initial diagnosis, problem escalation procedures, problem ticketing, problem logging, assignment of priority, and the ability to search through previous problems to find resolutions for new problems. A clear, quick, and effective escalation path is critical to DHHS for this system.

When issues arise, those issues are either recorded by submitting a project issue report inside of the Sandbox VisualVault environment or by communicating the issue to the project manager. When submitting a project issue inside of VisualVault, the submitter has the ability to identify severity as a means to prioritize the issue. When the issue is submitted, the implementation team will be notified of the issue via email and a task within VisualVault. The implementation team then will triage the issue and determines a plan of action to resolve the issue. The plan is scheduled amidst other issues in the project issue log, organized by priority. As issues are resolved, the implementation team mark the project issue as complete. Customer staff will receive an email prompting them to validate that the issue is resolved.
Customers can escalate issues by communicating with the project manager or VisualVault account representative.

Our approach and plan for support when the Department is fully in production follows. Included are recommendations for the service level agreement, and target response times.

VisualVault Post Implementation Support with Service Level Agreements (SLA)

1. On Call Support

1.1. The Principal Period of Support ("PPS") is a ten (10) hour contiguous daily time period between the hours of 8:00 AM and 6:00 PM, Eastern US local time, Monday through Friday, excluding VV's published holidays or holidays as observed locally by VisualVault. All Support subsequently added will have the same PPS.

2. Twenty-four (24) hour premium support services are available upon request and at an additional charge. Extended coverage options are subject to VisualVault's approval and the prevailing terms, conditions and prices for service at that time. Extended Hours Entitlement extends the Client's ability to place problem calls to VisualVault's Technical Services Group ("TSG") during the extended hours of coverage period and receive the same priority remote response for critical issues as during the PPS.

2. Severity Levels

Based on communications between Subscriber and VisualVault, the parties shall determine, in accordance with the following table, the "Severity Level" of each issue:

Severity Level	Definition
1	An issue that causes the Software to crash or be unavailable for use and which has no acceptable work-around.
2	An issue that affects multiple users of the Software and prevents effective use of an essential feature or essential features of the Software, but which does not cause the Software to be unavailable for use in whole.
3	An issue that affects productivity or ease of use of the Software and for which there is typically a work around.
4	An issue that does not materially affect Subscriber's (or any Subscriber Customer's) ability to use the Software (e.g., user interface inconveniences).

Based on the "Severity Level" of the issue, VisualVault and Subscriber shall take the following actions:

Severity Level	VisualVault Responsibilities	Client Responsibilities
1	Acknowledge and begin addressing immediately. VV's Client support and production	Call at time of discovering issue (email not acceptable for Severity 1). Be available to

	support teams will work continuously until fixed, 24x7 if not resolved by the close of the business day. Such 24x7 effort to commence first business day after determination of severity. Target resolution time is four (4) hours.	answer questions, provide information, and receive and install code fix immediately, 24x7 if not resolved by the close of the business day.
2	Acknowledge and begin addressing promptly. VisualVault's Client support and production support teams will work continuously within normal business hours until resolved. Target resolution time is 24 hours.	Be available to answer questions, provide information within four (4) hours of request. Install/test fix providing feedback.
3	Acknowledge within one business day. Issue will be scheduled to be addressed, based on the priority set by Client and VV. Target resolution time is seven (7) days.	Provide information and answer questions within one (1) business day.
4	Acknowledge within one business day. Issue will be addressed when possible, based on the priority set by Subscriber and VisualVault.	Provide information and answer questions within three business days.

Service Level Commitments

Commencing on the effective date of the applicable Subscription Period, VisualVault will provide to Customer the Service Level Commitments and Support Services defined herein as specified in the applicable Order. In the event of a conflict between the terms of the Agreement and the terms of this Exhibit B, the terms of this Exhibit B shall prevail.

Exhibit Definitions

"Downtime" means any period during which the Customer in unable to access or use the VisualVault Service because of an Issue, excluding (i) Scheduled Downtime or (ii) document preview, search, email uploads, sync or FTP functions of the VisualVault Service.

"Issue" means a single, reproducible issue or problem materially or significantly affecting the functionality of the VV Service.

"Scheduled Downtime" means a time period identified by VisualVault not to exceed 1 hour per calendar quarter and subject to 24 hours' prior notice wherever practical as provided to VV's general customer base, in which VV intends to have any downtime of the VisualVault Service or related systems.

"SLC Credit" means the credit identified in Section 3 below, which may be offered to Customer in the event Customer reports an Uptime Percentage of less than 99% where Customer has paid VisualVault for Premier Support for the applicable Account Licenses during the Subscription Period.

"Uptime Percentage" means the total number of minutes in a calendar month minus the number of minutes of Downtime suffered in such calendar month, divided by the total number of minutes in such calendar month.

2. Scope of Service Level Commitments

VisualVault's obligations do not extend to Issues or errors caused by:
(a) Third party hardware or software;
(b) Use of the VisualVault Service in violation of the terms of the Agreement;
(c) Use of the VisualVault Service other than in accordance with any user Documentation or the reasonable instructions of VisualVault;
(d) Third party hardware or software;
(e) Ongoing test or training instances of the VisualVault Service provided to Customer; or
(f) Services, circumstances or events beyond the reasonable control of VisualVault, including, without limitation, any Force Majeure events, the performance and/or availability of local ISPs employed by Customer, or any network beyond the demarcation or control of VisualVault.

3. Scheduled Downtime and Guaranteed Up Times

VisualVault will use commercially reasonable efforts to provide at least 24 hours' prior notice before implementing any .heduled Downtime. Subject to Customer's purchase of Premier Support, VV will provide Customer with the SLC Credits identified below during the applicable Subscription Period upon Customer's written request. The SLC Credit will be equal to the credit percentage identified in the table SLC Credits table below multiplied by the Customer's fees paid to VisualVault for the VisualVault Service that are attributable to the corresponding month (calculated on a straight line pro-rated basis with respect to any fees paid in advance). Customer will submit a written SLC Credit request to VV within 15 days of such Downtime. The SLC Credit is Customer's sole and exclusive remedy for any failure by VisualVault to meet any support obligations as identified herein.

Uptime Percentage	SLC Credit Percentage
Less than 99% but more than 98%	5%
Less than 98% but more than 97%	10%
Less than 97% but more than 96%	15%
Less than 96% but more than 95%	20%
Less than 95%	25%

The VisualVault implementation team begins to work with our customer support and training staff when UAT testing begins. We conduct internal meetings to begin to transfer knowledge to both teams. Our training group uses the information to build training modules. Our support team begins to learn the specifics of the LES system.

After go live, and for the next 30 days, our implementation leaders and support teams work jointly to address issues as they arise. After 30 days, our implementation team phases out of the project and the support team takes over full responsibility.

PROBLEM RESOLUTION (9.3)

The contractor shall continue to receive, record, and track problem reports and modification requests from users and provide feedback to users. Wherever problems are encountered, the problems shall be recorded and entered into the problem resolution process. The contractor shall provide interactive support for users to report system problems.

VisualVault will maintains and will provide the following process for issue resolution:

1. Issues are reported based upon the agreed upon support process.
2. Issue is triaged for root cause and potential resolution.
3. Issue is assigned to an appropriate support level:
    a. Level 1 resolves issues with VisualVault that are not solution specific. Resolves rudimentary issues that can be resolved with the solution.
    b. Level 2 resolves solution issues that are solution specific.
    c. Professional Services or Level 3 resolves issues related to business rules, scripts or integrations
    d. Developers resolve issues relating to complicated scripts, integrations or VisualVault product.
4. Testing of the resolution occurs in Development and Sandbox environments.
5. Customer tests and approve resolutions in the Sandbox environment.
    a. Approval will initiate the next change control step.
    b. Denial sends the issue back to step 3.
6. Change control facilitates identifying a date and migration plan.
7. Customer approves change control.
8. On the approved data, resolution placed in production and tested to ensure appropriate configuration.

DELIVERABLES

The awarded contractor's system shall deliver the following documents and activities that meet with DHHS approval. The Bidder shall submit a Deliverable Schedule detailing the number of weeks each deliverable will require from beginning to completion and the payment percentage of the total project cost of each deliverable, not including on-going O&M annual fees or licensing fees. Under no circumstances shall the sum percentage of deliverables prior to completion of implementation exceed 35%. The deliverables prior to Implementation are Project Planning, Requirements Analysis Design, Development, Interfaces and Integration, Data Conversion, Testing, and Training.

Milestone	Payment Percentage of Total Project Cost (not including on-going O&M annual fees or licensing fees)	Due Date

Development, Interfaces and Integration		
Data Conversion		
Training		
	100%	

Project Planning
Detailed Project Work Plan
Testing Methodology
Risk Management, Issue Management, and Organizational Change control, Work Management, Change Control procedures
Status Reporting Plan
Project Status Meetings Protocol
Electronic Project Library
Security Plan
Business Continuity Plan/Disaster Recovery Plan
Requirements Analysis
Requirements Validation Documents
Fit/Gap Analysis
Pilot/Prototype
Design
Detailed System Design Documentation
Testing Plan
Development, Interfaces, and Integration
Software Development Plan
Development/Customization
Software Development Summary Report
Schedule of Interface Development Efforts
Interface Environment Setup
Interface Development and Testing
Data Conversion
Data Conversion Plan and Guide
Conversion Results Report
Testing
User Acceptance Plan and Testing
User Acceptance Testing Results
Training
Training Plan
Training Sessions
Video Sessions
Training Manuals

Implementation
Implementation Plan
Final Readiness Assessment
Documentation
Problem Resolution Plan
System Go-Live

Operations and Maintenance

VisualVault will comply with these requirements and do so as a standard practice.

PLANNING - TRAINING PLAN - SECTION 7.1 SOW

Our planning will include configuration specifically for Nebraska's SUA Aging Information System Software needs, including Nebraska Aging Management Information System (NAMIS) replacement, case management and services (Mediware@, SAMS), and an information and referral database. client services, care and case management, funding splits, administration requirements, and federal reporting requirements.

Our planning efforts will be guided by a Training Plan which will define required training, define the process for delivering the training, & define the stakeholders who will receive the training. We recommend that Nebraska SUA's Training Plan also incorporate Knowledge Transfer activities–those that define the process for transferring system and technical knowledge/information to the appropriate staff.

The Training Plan will specify tasks, methods, materials, and timelines regarding use of our Solution in the following areas:

- Initial understanding, navigation, and use for all *involved in the defined processes*
- Initial understanding, navigation, for *"train the trainer"* team members
  Initial understanding, navigation of the system for *SUA staff*
  Initial understanding, navigation of the system for e*xternal stakeholder/partner users*
- Initial understanding, navigation of the system for System Administrators (SAs)
- Master VisualVault use for all, including SAs
- Leadership training to familiarize each on navigation, use, with a keen focus on reports and how to use them to improve performance and how to track service improvement
- Use of dashboard and reports to document the expected 15% up to 25% reduction in staff labor hours dedicated to NAMI documentation activities.

The Training Plan will provide the necessary structure and processes for SUA and its stakeholders/partners to develop the knowledge, skills, and abilities necessary to operate our Solution. We recommend submission of a Training Completion and Knowledge Transfer Acknowledgement Report to confirm delivery and completion of transition to SUA operation.

DEVELOPMENT

VisualVault's training is designed for the different user groups who have varying education requirements based on system use. We develop our training to maximize the user experience by gaining the knowledge required to transform their workday. We develop training strategies that seek to enhance the student's learning experience by incorporating active learning techniques and leveraging SUA Subject Matter Experts (SMEs). This methodology, which is based on best practices and proven experience, is clear and well-defined to minimize risk and enhance communications of risk items and action plans.

Our training is based on adult learning principles and inclusive of a variety of learning styles. We develop training based on some assumptions about how adults learn (Malcolm S. Knowles):

- Adults want to know why they should learn.
  Adults need to take responsibility.
  Adults bring experience to learning.
- Adults are ready to learn when the need arises.
- Adults are task-oriented.

And adults have different learning styles–visual, auditory, and experiential/kinesthetic. Research confirms that we retain approximately 10% of what we see (visual), 30-40% of what we see and hear (visual and auditory), and 90% of what we see, hear, and do (visual, auditory, and experiential). Our proposed training methods address these issues and include readings, videos/slides, lectures, group discussions, examples, role plays, and practice demonstrations–all three learning styles. Our training types have included on-site classroom curriculum, instructor-led, self-paced and self-study, web-based live and recorded sessions for "external" community users (which we have found to be particularly effective for providers), mobile functionality & use of iForms off-line for field inspectors and investigators, and onsite or remote refresher training. We are accustomed to conducting training on policy and/or business process changes, application builds or releases, special or infrequent procedural updates, gap identification and remediation, and training for leadership on navigation and report use. Materials and manuals (Section 7.4 SOW) to support our training efforts can be customized based on SUA needs and can be provided via web portal, CD, or other appropriate method. Training manuals including an online Quick Reference Guide will be provided documenting the use of the VisualVault solution. This manual will be used in conjunction with the Solutions Training classes listed below. This manual will serve as documentation for how the solution operates at the time it is implemented.

Thus, we use a wide variety of training methods:

- On-site classroom curriculum
- Instructor-led
- Self-Paced and Self-Study
- Web based live and recorded sessions for "external community users such as Providers
- Particularly effective for provider education
- A portion of the training is designed for field inspectors and investigators to use VisualVault mobile functionality and how to use iForms off-line
- Refresher training can be scheduled and performed onsite or remotely
- Policy and/or Business Process changes
- Application Builds or Releases

- Special or Infrequent procedural updates
- Gap identification and remediation.

We customize our training to fit the needs of our customers. Our experience has led us to categorize our training based the following target audience:

- Mandatory - contractually required for assignment to the project [i.e. HIPAA, Security, Fraud, Waste and Abuse, Rights and Responsibilities, etc.]
- Functional Role/Job Specific - to perform a job or function [i.e. system navigation, processing of various submitted materials, complaint reviews, case tracking, etc.
- Supervisory or Lead - team operations and management
- System Administrative - Learning how to navigate, resolve minor issues, make changes to iForms, workflows, etc.
- Leadership - Educate management on navigation and report use.

DRAFT PROJECT WORK PLAN

Task Name	Duration	Start	Finish
NE Aging Information System Software Solution	**171.96 days**	**Fri 3/1/19**	**Fri 11/1/19**
Contract Execution	1 day	Fri 3/1/19	Fri 3/1/19
Project Planning - Project Management	**156.28 days**	**Mon 3/4/19**	**Fri 11/1/19**
Requirements Analysis - Deliverable 2	**38.63 days**	**Mon 3/11/19**	**Thu 5/2/19**
Design - Deliverable 3	**12.42 days**	**Mon 4/1/19**	**Thu 4/18/19**
Configuration / Development - Deliverable 4	**93.25 days**	**Tue 4/2/19**	**Tue 8/13/19**
Data Conversion / Migration (Deliverable 5)	**126.81 days**	**Thu 3/14/19**	**Thu 9/12/19**
Testing - Deliverable 6	**26.76 days**	**Mon 8/26/19**	**Thu 10/3/19**
Training - Deliverable 7	**23.75 days**	**Mon 8/26/19**	**Mon 9/30/19**
Data Migration/Integration - NE "Implementation" - Deliverable 8	**142.81 days**	**Thu 4/11/19**	**Fri 11/1/19**

Task Name	Duration	Start	Finish
NE Aging Information System Software Solution	**171.96 days**	**Fri 3/1/19**	**Fri 11/1/19**
Contract Execution	1 day	Fri 3/1/19	Fri 3/1/19
Project Planning - Project Management	**170.09 days**	**Mon 3/4/19**	**Fri 11/1/19**
Project Management - Initiation	**16.63 days**	**Mon 3/4/19**	**Tue 3/26/19**
Quarterly Project Management	**66 days**	**Mon 3/18/19**	**Wed 6/19/19**
Quarterly Project Management	**61 days**	**Mon 6/24/19**	**Thu 9/19/19**
Project Management – Close-Out	**26.34 days**	**Tue 9/24/19**	**Fri 11/1/19**
Requirements Analysis - Deliverable 2	**38.63 days**	**Mon 3/11/19**	**Thu 5/2/19**
Discovery	**3.5 days**	**Mon 3/11/19**	**Thu 3/14/19**
Requirements Specifications	**28.5 days**	**Fri 3/15/19**	**Thu 4/25/19**
Form specifications	**10.87 days**	**Mon 3/18/19**	**Mon 4/1/19**
Business logic & validation script specifications	**1.5 days**	**Mon 3/18/19**	**Tue 3/19/19**
Report specifications	**2.05 days**	**Mon 3/18/19**	**Wed 3/20/19**
Search specifications	**0 days**	**Fri 3/15/19**	**Fri 3/15/19**
UI (portal screen) specifications. 6 Roles	**0.38 days**	**Mon 3/18/19**	**Mon 3/18/19**
Requirements Validation Document	13.25 days	Mon 4/1/19	Fri 4/19/19
Fit / Gap Analysis	13.25 days	Mon 4/1/19	Fri 4/19/19
Requirements Specifications Document	7.29 days	Mon 4/1/19	Thu 4/11/19
Pilot / Prototype	17.64 days	Mon 4/1/19	Thu 4/25/19
Acceptance	**5.13 days**	**Thu 4/25/19**	**Thu 5/2/19**
Design - Deliverable 3	**12.42 days**	**Mon 4/1/19**	**Thu 4/18/19**
Detailed System Design Documentation	7.29 days	Mon 4/1/19	Thu 4/11/19
Testing Plan	6.79 days	Mon 4/1/19	Wed 4/10/19

Acceptance	5.13 days	Thu 4/11/19	Thu 4/18/19
Configuration / Development - Deliverable 4	93.25 days	Tue 4/2/19	Tue 8/13/19
4.1 Plan, Schedule, Environment Set-Up	8.58 days	Tue 4/2/19	Mon 4/15/19
Development / Customization	74 days	Thu 4/11/19	Fri 7/26/19
4.2 Core Processes	14 days	Thu 4/11/19	Wed 5/1/19
4.3 Client Services - CLI-1 to CLI-18	10 days	Mon 4/29/19	Mon 5/13/19
4.4 Services - SER-1 to SER-19	10.42 days	Thu 5/9/19	Thu 5/23/19
4.5 Assessments ASMT-1 to ASMT-14	15.77 days	Wed 5/22/19	Thu 6/13/19
4.6 Usability USE-1 to USE-13	5.04 days	Wed 6/12/19	Wed 6/19/19
4.7 Fiscal FIS-1 to FIS-9	5.63 days	Fri 6/14/19	Fri 6/21/19
4.8 Reporting REP-1 to REP-15	13.67 days	Thu 6/20/19	Wed 7/10/19
4.9 Volunteer Management VOL-1 to VOL-2	3.52 days	Thu 7/11/19	Tue 7/16/19
4.10 Provider Information PRV-1 to PRV-5	3.38 days	Mon 7/15/19	Thu 7/18/19
4.11 Operations OPR-1 to OPR-7	7 days	Wed 7/17/19	Fri 7/26/19
4.12 Reports / UI	3.83 days	Fri 7/26/19	Wed 7/31/19
4.13 Configuration Close-Out	78.79 days	Tue 4/23/19	Tue 8/13/19
Data Conversion / Migration (Deliverable 5)	126.81 days	Thu 3/14/19	Thu 9/12/19
Data Conversion Plan & Guide - 5.1	88.87 days	Thu 3/14/19	Fri 7/19/19
Data Conversion Environment - 5.2	17.42 days	Wed 7/31/19	Mon 8/26/19
Conversion Results Report - 5.3	6.79 days	Mon 8/26/19	Thu 9/5/19
Acceptance	5.13 days	Thu 9/5/19	Thu 9/12/19
Testing - Deliverable 6	26.76 days	Mon 8/26/19	Thu 10/3/19
Unit, System, Interface Test Plan - 6.1	1.99 days	Thu 9/5/19	Mon 9/9/19
Conduct Unit Testing	11.96 hrs.	Mon 9/9/19	Tue 9/10/19
Conduct Internal System Testing	11.96 hrs.	Tue 9/10/19	Thu 9/12/19
Conduct Interface Testing	11.96 hrs.	Thu 9/12/19	Fri 9/13/19
User Acceptance Plan & Testing	26.76 days	Mon 8/26/19	Thu 10/3/19
UAT Plan - 6.1	16.5 days	Mon 8/26/19	Wed 9/18/19
Testing - 6.2	3.13 days	Wed 9/18/19	Tue 9/24/19
Acceptance	7.13 days	Tue 9/24/19	Thu 10/3/19
Training - Deliverable 7	23.75 days	Mon 8/26/19	Mon 9/30/19
Training Plan (4 strategies, 2 approaches) - 7.1	7 days	Mon 8/26/19	Thu 9/5/19
Training Documentation	3.75 days	Mon 8/26/19	Fri 8/30/19
Conduct Training Sessions	14.88 days	Fri 8/30/19	Mon 9/23/19
Training Manual - 7.4	1.79 days	Thu 9/5/19	Mon 9/9/19
Acceptance	5.13 days	Mon 9/23/19	Mon 9/30/19
Data Migration/Integration - NE "Implementation" - Deliverable 8	142.81 days	Thu 4/11/19	Fri 11/1/19
Implementation Plan - 8.1 - includes Problem Resolution Plan	69.34 days	Thu 4/11/19	Fri 7/19/19
Integration / Interfaces - 8.2	16.87 days	Fri 7/19/19	Tue 8/13/19
Data Migration - 8.3	33.53 days	Tue 8/13/19	Mon 9/30/19
Test Migrations (Mock Data Conversion Iterations)	72.22 hrs.	Tue 8/13/19	Mon 8/26/19
Migrations	5.12 days	Mon 8/26/19	Tue 9/3/19
Final Readiness Assessment (Checklist)	0.25 days	Tue 9/24/19	Tue 9/24/19
Deployment to Production	19 hrs.	Thu 9/26/19	Mon 9/30/19
System Go-Live	0.5 days	Mon 9/30/19	Mon 9/30/19
Documentation - 8.4	10.94 days	Mon 9/30/19	Wed 10/16/19
Acceptance	12.13 days	Wed 10/16/19	Fri 11/1/19

Attachment B
Business Requirements Traceability Matrix
Request for Proposal Number 5948 Z1

Bidders are instructed to complete a Business Requirements Traceability Matrix for Aging Services software replacement. Bidders are required to describe in detail how their proposed solution meets the conformance specification outlined within each Business Requirement.

The traceability matrix is used to document and track the business requirements from the proposal through testing to verify that the requirement has been completely fulfilled. The contractor will be responsible for maintaining the contract set of Baseline Requirements.

The traceability matrix should indicate how the bidder intends to comply with the requirement and the effort required to achieve that compliance. It is not sufficient for the bidder to simply state that it intends to meet the requirements of the RFP. DHHS will consider any such response to the requirements in this RFP to be non-responsive and the bid may be rejected. The narrative should provide DHHS with sufficient information to differentiate the bidder's business solution from other bidders' solutions.

The bidder must ensure that the original requirement identifier and requirement description are maintained in the traceability matrix as provided by DHHS. Failure to maintain these elements may render the bid non-responsive and result in for rejection of the bidder.

How to complete the traceability matrix:

Column Description	Bidder Responsibility
Req #	The unique identifier for the requirement as assigned by DHHS, followed by the specific requirement number. This column is dictated by this RFP and must not be modified by the bidder.
Requirement	The statement of the requirement to which the bidder must respond. This column is dictated by the RFP and must not be modified by the bidder.
(1) Comply	The bidder should insert an "X" if the bidder's proposed solution complies with the requirement. The bidder should leave blank if the bidder's proposed solution does not comply with the requirement. If left blank, the bidder must also address the following: • Capability does not currently exist in the proposed system, but is planned in the near future (within four months from the date of submission of the bid) • Capability not available, is not planned, or requires extensive source-code design and customization to be considered part of the bidder's standard capability • Requires an extensive integration effort of more than 500 hours

Column Description	Bidder Responsibility
(a) Core	The bidder should insert an "X" if the requirement is met by existing capabilities of the core system or with minor modifications to existing functionality.
(b) Custom	The bidder should insert an "X" if the bidder proposes to custom develop the capability to meet this requirement. Indicate "custom" for those features that require substantial or "from the ground up" development efforts.
(c) 3rd Party	The bidder should insert an "X" if the bidder proposed to meet this requirement using a 3rd party component or product (e.g., a COTS vendor, or other 3rd party). The bidder must describe the product, including product name, its functionality and benefits in their response.

1. State Unit on Aging requirements:
   a. Clients

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
CLI-1	Describe how software creates a focus on the person receiving the services instead of focus on the services.	X			
	Bidder's Response: When the Nebraska's Department of Health and Human Services (DHHS) reads and understands the value and benefits gained from our Unique Community Licensing and technology platform, you will agree that the VisualVault solution is designed with the focus on elders qualifying for care and services. Legacy client management systems are document centric. VisualVault's client management plafform is designed with a focus on the individual with all information organized around the individual's profile form and the provided services. VisualVault's solution is named Elders First because the fact is, the purpose of the new Aging Information System (AIS) is to enable the community involved in every aspect of 'client' services to perform their responsibility to the program more effectively culminating in improved outcomes and overall care delivery. Please review our executive summary and Community Licensing and how it aligns precisely with this goal. From a data and process standpoint, the Elders First solution is oriented around the client. The platform is highly configured to integrate information across services to allow agencies to see the entire picture for each citizen served.				
CLI-2	The system must have a unique identifier (client number) for client records besides Social Security Number.	X			
	Bidder's Response: The VisualVault solution fully complies with this requirement. VisualVault will create a unique Identifier Number for each case and use that initial number to link all additional documentation and data to the original case file.				
CLI-3	The system must be able to manage and identify possible duplicate clients, merge clients, and client creation.	X			
	Bidder's Response: Core to VisualVault is the capability to run validation checks automatically based on DHHS business rules.				
CLI-4	The system must collect all National Aging Program Information System (NAPIS) required demographic fields in the client record.	X			
	Bidder's Response: Core functionality. VisualVault will use of IForms to list each NAPIS demographic field. Business rules will be used to make each field required to assure it has been filled in. Business rules will validate each field to assist in assuring the data is accurate. Across all the client services functions, we have assumed automation of 5 iForms with an average of 50 fields each, one iForm with 100 fields, 6 key processes, and the supporting reporting for these iForms and processes. During the discovery and requirements work, the team will work with your users to capture the detailed requirements which will be configured to customize the Elders First Solution.				
CLI-5	The state must be able to add additional (ad-hoc) fields added to the client record to track non-Older Americans Act (OAA) information.	X			

	Bidder's Response: Core functionality. VisualVault's use of iForms to add data makes this requirement very simple. Please see the graphic of our iForm template builder that the system administrator will use to drag and drop new fields whenever required.				
CLI-6	The system must accommodate adding new fields post implementation.	X			
	Bidder's Response: Core functionality. VisualVault's use of iForms to add data makes this requirement very simple. Please see the graphic of our iForm template builder that the system administrator will use to drag and drop new fields whenever required.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
CLI-7	The system must include and track federal Activities of Daily Living (ADLs) and Instrumental Activities of Daily Living (IADLs) for each client.	X			
	Bidder's Response: Core functionality. VisualVault will use workflow business rules to track ADLs and IADLs for each client. Tracking of any data point is standard functionality.				
CLI-8	The system must provide historical values for client ADL and IADL indicators.	X			
	Bidder's Response: Core functionality. At the heart of VisualVault platform is a mature Enterprise Content Management (ECM) services suite. All documents and data submitted to VisualVault are assigned a classification, naming convention, unique ID, etc. to link the content to the correct virtual case. VisualVault is a true archive and all content once submitted cannot be changed or deleted. New or revised documentation is attached as a revision to the original document(s) to assure the legality of the file.				
CLI-9	The system must differentiate between "not answered" and "no" for ADL and IADL responses.	X			
	Bidder's Response: Core functionality. This requirement uses standard iForm functionality and DHHS business rule(s). VisualVault continually audits required fields and the response within the field to ensure an answer has been inputted.				
CLI-10	Describe how the system would accommodate ADLs that are different from the federal ADLs.	X			
	Bidder's Response: VisualVault will work with DHHS to identify all state ADLs and Federal ADLS and mark each as such. Then depending upon who has logged in and the client being assessed, VisualVault will use DHHS business rules to determine which data fields need to be populated.				
CLI-11	The system must include a way to manage client status, including but not limited to: active, inactive, and deceased clients.	X			
	Bidder's Response: Core Functionality. VisualVault can address this several ways. The easiest is to have a drop-down list of the three types. When one is selected, the status is in force. If the status changes, based on security rights, an authorized user can select another status and immediately the status would be updated. Security would decides who is allowed to change this information.				
CLI-12	The system must track the care recipient to caregiver relationship with separate client records. Client records can be setup based on roles. Recipients can be setup as such with caregivers, service providers, etc. setup under their own group classification. Caregivers and service providers can be members of multiple groups and VisualVault will track each independently but show the relationship on the user's dashboard.	X			
	Bidder's Response: Core functionality. VisualVault stated earlier that we classify each document and use the unique ID or other unique identifier to link documents to the original case file. The same process will be used to link one or more caregivers to a client. Clients can be a "one to many" regarding individuals and groups included in their program.				
CLI-13	Describe how the system tracks out of state caregivers.	X			

	Bidder's Response: There are multiple ways for VisualVault to track our of state caregivers. A simple solution is for VisualVault will include a 'state' field on the caregiver's profile/application iForm. Once the field is populated, tracking the caregiver by state is achieved.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
CLI-14	The system must be able to manage emergency and other contact information including but not limited to contact name, relationship, and contact information.	X			
	Bidder's Response: This information will be configured using the iForms during the system implementation.				
CLI-15	The system must contain a section that allows users to input observations, notes, follow ups, and other text-based summaries in the client record. All notes must be saved chronologically in a historical log (not over-written with the next update).	X			
	Bidder's Response: Core VisualVault functionality. VisualVault iForms will be configured to accommodate notes, text-based summaries, etc. To configure this, VisualVault will use the iForm template to drag and drop the note fields area onto one or multiple locations within the form.				
CLI-16	The system must be able to have multiple files/documents attached to a client record.	X			
	Bidder's Response: Core VisualVault functionality. At the core of VisualVault is our ECM services suite designed to manage documents and meta data. Uploading documents can be achieved by simply drag and dropping one or multiple files/documents and will be auto linked to the associated file.				
CLI-17	Describe how an area agency on aging (AAA) would transfer a client to another AAA in the system.	X			
	Bidder's Response: Core VisualVault functionality. Multiple approaches to achieve this. One way is to have a drop-down list of AAAs. The original AAA will be selected. When a client is to be transferred, an authorized users could simply click on the drop down list, select the new AAA and the transfer occurs. Various security can be wrapped around this function to assure only authorized users may make this change. Additionally, every change to the system/record is automatically captured in the background providing a complete audit trail of changes. This data will be posted on the appropriate person's dashboard and can be used to populate reports.				
CLI-18	List fields that users at the AAA or State Unit on Aging (SUA) level can search by. List any additional fields that would be considered a customization to the standard search fields.	X			
	Bidder's Response: Once the system is configured, any field and part of data set can be searched.				

b. Services

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SER-1	The system must be able to track federal, state, and local taxonomies. Describe how the system reconciles different taxonomies. Describe how the system incorporates the AIRS taxonomy.	X			
	Bidder's Response: The Elders First platform fully meets this requirement. There are options to address this requirement. • AIRS gives us their format and we can import it. • We configure a drop down of AIRS taxonomy and Index each item according to all applicable taxonomies. We then can cross reference the others • Import all taxonomies to build a cross reference list through index fields				
SER-2	The system must be able to differentiate between Aging and Disability Resource Center (ADRC) services and OAA services..	X			
	Bidder's Response: VisualVault has a robust repository and maintains all data and supporting content. VisualVault will create a database of services and track whether the services are being provided by ADRC or OAA.				
SER-3	The system must be able to distinguish between service delivery models: self-directed care services and traditionally delivered services.	X			
	Bidder's Response: VisualVault establishes service libraries for each model using our iForms to capture the individual services. The platform uses the services list to validate and classify the service when it is entered on all subsequent work.				
SER-4	The system must be able to do rapid or bulk data entry by service and service provider (i.e. entering daily congregate meal recipients at a senior center).	X			
	Bidder's Response: Core VisualVault functionality. VisualVault's ECM design provides for individual and bulk data entry by services or any other criteria.				
SER-5	Describe how the system handles canceling or rescheduling authorized services due to inclement weather or other unforeseen circumstances.		X		
	Bidder's Response: VisualVault will use the integrated calendaring function for staff to reschedule.				
SER-6	Describe how the system tracks OAA registered service recipients before an intake is received.	X			
	Bidder's Response: VisualVault will use an iForm to register all OAA recipients. Once registered, the Elders First platform tracks any action or activity associated to the record prior to an intake being received.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SER-7	Describe how the system administers or customizes eligibility types. Eligibility will differ between various state and federal programs.	X			
	Bidder's Response: iForms are the vehicle that the platform uses to collect data. Each eligibility type will be identified using iForms business rules and will be configured for each. As additional data is required per "type" or a new "type" is required, the administrator simply drags and drops the new data fields onto the form, applies the business rule, and if a completely new type is required, the administrator will be trained to setup a new iForm.				
SER-8	The system must be able to track services received by non-OAA eligible individuals.	X			
	Bidder's Response: VisualVault uses business rules and iForms to establish what services are administered to non-OAA eligible individuals. VisualVault was originally designed to be a compliance tool for the medical manufacturers. As such, every activity occurring within the system is recorded and is used to track.				
SER-9	The system must include historical eligibility tracking. For example, a 59 year old person can join their 60 year old spouse for an OAA Congregate Meal. Once the 59 year old spouse turns 60, they would qualify for OAA Congregate Meals.	X			
	Bidder's Response: Your business rules will be used to trigger changes within the platform. Notifications can also be triggered to alert the recipient and staff that a change has occurred. Reports will be auto generated to track these changes as well for review.				
SER-10	The system must track special diets and delivery notes required for Home Delivered Meal service.	X			
	Bidder's Response: Notes fields on iForms are used to input information. VisualVault could also create a drop down list of the most common diets. The user would simply select the field and then enter the associated notes in the note section.				
SER-11	Describe how the system would track take-out meals that are taken off senior center/nutrition site premise.	X			
	Bidder's Response: An iForm would be created to track nutrition information. This iForm will auto link to the client's case file. All nutrition information that DHHS requires will be entered onto this form. All data is uploaded to the case files and can be viewed via the dashboard interface.				
SER-12	Describe the system's electronic visit verification capabilities (EVV).	X			
	Bidder's Response: This is a strength of the VisualVault platform. VisualVault uses an iForm to collect all data. These forms function when on-line or off-line. Each field can be configured with the proper business rule to verify data being entered and validated. The form provides an immediate notification telling the individual that the data entered is not appropriate and allows the person to make the change. Business rules can also be used to not allow the form to be submitted if fields are empty or fields with errors are not corrected.				
SER-13	Describe the system's routing capabilities for services like transportation and home delivered meal routing. Include a description of GIS mapping, monitoring from a central location, etc.	X			
	Bidder's Response: VisualVault's workflow is used to auto route documents and forms to the appropriate person or team. Document classification assists in the auto routing. VisualVault has integrated with leading GIS systems such as Esri. When integrated, GPS can be used to help with scheduling and to locate addresses.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SER-14	Describe how the system automates and customizes workflows to determine client eligibility for services. Describe how it can be customized by AAA and service.	X			
	Bidder's Response: VisualVault's workflow is core functionality. DHSS business rules are used to customized the workflow to support each process. Business rules within iForms and workflow can be used to determine if all information has been completed and based on the answers, is eligible or not. Based on that determination, workflow will be configured to route the content to the appropriate inbox. Notifications to the submitting party will be generated informing them of the status. Denied eligibility can be returned to the submitter's inbox to make changes. Approved submittals are routed to the next review stop.				
SER-15	Describe how the system automates and customizes waitlist and prioritization capabilities post system implementation. Describe how it can be customized by AAA and service.	X			
	Bidder's Response: This is a strength of the VisualVault solution. Community Licensing enables all participants to have a license and work within the system. One of the benefits is those who are on waitlists can Self-Serve to determine their status at any time. They log in and see their status and position on the waitlist and the system can provide an estimated length of time it will take.				
SER-16	Post implementation, describe the system customizable prior authorization forms. Describe how it can be customized by AAA and service.	X			
	Bidder's Response: This requirement is a strength of VisualVault. Prior authorization forms will be created using VisualVault iForm template builder. The template builder is a drag and drop tool enabling a trained staff person to easily create forms and make changes to forms as requirements evolve. Each form can be opened and changed (with proper security) based on the service and changes. VisualVault enables each form to have fields that cannot be altered except with leadership approval. The purpose of this approach is to assure required information is captured in the format while the other fields can be changed with proper security rights. (see iForm template builder graphic in the VisualVault response document)				
SER-17	Describe the system's real time data entry for information & assistance staff to track calls and walk-ins, where staff provide information and referral services.	X			
	Bidder's Response: VisualVault will present a screen where the walk-in or phone person can enter their name and any other information the state prefers. The system provides a queue on their dashboard. The time they signed in, the reason for the inquiry, etc. all can be presented. Additionally, VisualVault offers smart phone capability. When a call comes in, the VisualVault system intercepts the call and ask the individual if they would like to participate in a "visual" experience. If they select yes, a link is instantly sent to their phone. They click on the link and a list of options for them to choose is presented. They enter it and they can self-serve their needs. Much more can be explained however, the option for the Department to provide a visual self-service experience 24/7/365 establishes a new level of service for the department during work hours as well as after.				
SER-18	Describe how the system records anonymous clients, referrals made, and level of assistance provided.	X			
	Bidder's Response: VisualVault uses iForms to capture data. The iForm could have a drop-down field to designate if the client being onboarded should be anonymous or not (a simple Yes/No). All data entered on the iForm is captured, a unique ID is assigned, and all subsequent notes, uploaded support documents, etc. are auto linked using the ID number and or other unique metadata.				

SER-19	Describe how the system supports a "lending library" tracking system. For example, describe how the AAA would track durable medical equipment that has been lent to a client, including how it would be administered, such as donations of equipment, loaning, and marked returned and available for use.	X			
	Bidder's Response: VisualVault addresses this requirement with an iForm. Community Licensing enables the requesting party to log in and select the "Lender" iForm. They complete the form and can sign the form using VisualVault's eSignature. They click submit and the workflow routes the Lender iForm to the appropriate person to review and approve. Once approved, business rules will track and set triggers for the date the equipment is to be returned. An alert can be auto generated a set number of days prior to the return date to remind the person/company. When the equipment is returned, the form could have a simple check box marked "returned" and that would trigger the loan as closed. VisualVault tracks all the actions occurring with the iForm therefore, all actions are recorded and can be presented to the staff's dashboard and reports. All this functionality can also be performed using our smart phone capability enabling people/companies to perform all these tasks using their phone. Equipment donations can also be logged using an "Donation iForm." Once the form is submitted, workflow will route the information to the right staff for review and they can file the iForm in the appropriate digital folder or filing can be done automatically based on the iForm classification. Looking at your SER-1 through SER-19 requirements, we have assumed the configuration of 5 iForms with 30-50 fields each and 5 supporting processes and reports. These processes will be configured to your validation and workflow requirements.				

c. Assessments

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
ASMT-1	Describe how the State can create and customize assessments in the system.	X			
	Bidder's Response: This is a strength of the VisualVault solution. Our iForms are designed to be easily configured using the iForm template builder. The template builder is a drag and drop tool enabling trained system administrators to customize any iForm. The Assessment form functions online and offline enabling case workers/field staff to capture all information regardless of connectivity. Across ASMT1 – ASMT-14 requirements, we have assumed automation of one iForm with 600 fields, one iForm with 900 fields, and six iForms with an average of 200 fields. We have assumed each iForm has a corresponding workflow configuration, validation script, queries, and supporting reporting. Thus, the assessment processes are aligned with the Nebraska approach and unique needs and data requirements.				
ASMT-2	Describe how the system accommodates multiple value choices.	X			
	Bidder's Response: VisualVault typically configures iForms with multiple choices with drop down lists or boxes that enable a user to quickly choose one or multiple fields. This approach also enables a user with the appropriate user rights to change the selection in the future. System Administrators can change the field list when there is a change required.				
ASMT-3	Describe how the system aggregates collected data.	X			
	Bidder's Response: VisualVault uses our data analytics function and presents aggregated/repurposed data using dashboards and reports. We design and build the dashboards to show data sets. NE admins will be able to build and redesign dashboards to view new data requirements.				
ASMT-4	Newly created assessments must be available to previously created client profiles.	X			
	Bidder's Response: Assessment iForms are used to capture information. Meta data is prepopulated from data previously captured and resident within VisualVault or any 3rd party application that our platform is integrated with. VisualVault uses unique meta data to auto link new documentation to each client profile.				
ASMT-5	Describe how the system reconciles data in an old assessment and new assessment.	X			
	Bidder's Response: VisualVault was originally designed as a compliance tool for medical manufacturing. As such, any and all data fields can be validated as information is entered. Additionally, the system uses business rules to compare and reconcile data in old and new assessments and highlight discrepancies.				
ASMT-6	Describe how the system would retain previously deleted assessment questions.	X			
	Bidder's Response: VisualVault's secure repository is a true archive. Once an assessment has been saved to the repository, it cannot be changed. The assessment can be opened and changed but will be saved as a revision to the original to ensure the legality of the information. Previously deleted questions can be viewed on the previous assessment.				
ASMT-7	Describe how the system provides historical data and trending with previous assessment answers.	X			
	Bidder's Response: VisualVault has robust data analytic capability. All data is retained in the VisualVault repository. Queries are used to filter data and present results to the user dashboard and or a report. For example, every field on assessment forms can be queried and aggregated to proactively see trends.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
ASMT-8	The system must include the DETERMINE Assessment tool (from the Nutrition Screening Initiative) to evaluate nutrition risk. (**D**isease; **E**ating Poorly; **T**ooth Loss/Mouth Pain; **E**conomic Hardship; **R**educed Social Contact; **M**ultiple Medicines; Involuntary Weight Loss/Gain; **N**eeds Assistance in Self- Care; **E**lder Years Above Age 80).	X			
	Bidder's Response: This requirement can be supported with another iForm to include all questions involved in the DETERMINE Assessment tool. We assumed this iForm would contain a minimum of 100 fields to be created. Alternatively, we could integrate to the application to allow users to work within that system and save the results and data in both VisualVault and their application.				
de	The system must include the St. Louis University Mental Status (SLUMS) Assessment to evaluate cognitive performance.	X			
	Bidder's Response: This requirement can be supported with another iForm to include all questions involved in the St. Louis University Status Assessment tool. We estimate a thirty field iForm to automate this cognitive assessment.				
ASMT-10	Describe how the state care management assessment would be set up in the system. An example of the assessment can be found at this URL: http://dhhs.ne.gov/medicaid/Aging/Documents/CM%20Assessment%20Form.pdf	X			
	Bidder's Response: The state's care management assessment will be incorporated into the Elders First platform using the iForm template builder. If NE does not require any changes to the form, The VisualVault Team will use the template builder to configure this as is. We assumed approximately 275 fields to be configured to replicate this form in VisualVault. Once configured, your assessors would use the form as they do today however, the iForm functions online or offline and once submitted, can auto upload data from the form directly to any third-party systems as well as the all data fields are immediately available for analytic work and presentation on user dashboards. VisualVault offers a no wrong door approach. A user who logs in will simply look in the forms list, find this and fill it in and submit. Workflow would auto route it based on the document classification. The care management assessment can also be placed on the Department's website, downloaded, completed and either saved and submitted via an email or printed and mailed in. An individual can also complete the form and bring it to a local office.				
ASMT-11	Describe how the state would administer and customize a caregiver assessment form in the system. The assessment can be found online at: http://dhhs.ne.gov/medicaid/Aging/Documents/SUA-18-IM-04%20Comprehensive%20Caregiver%20Assessment.pdf	X			
	Bidder's Response: This is core VisualVault functionality. The state's caregiver assessment created using the iForm template builder. If NE does not require any changes to the form, The VisualVault Team will use the template builder to configure this as is. The state may customize any iForm by having the system administrator open the template builder, select the form to be updated, and drag and drop new fields onto the form and name them. System administrators are trained to create new iForms and to change existing ones. VisualVault offers a no wrong door approach. A user who logs in will simply look in the forms list, find this and fill it in and submit. Workflow would auto route it based on the document classification. The caregiver management assessment can also be placed on the Department's website, downloaded, completed and either saved and submitted via an email or printed and mailed in. An				

	individual can also complete the form and bring it to a local office.				
ASMT-12	Describe how the system supports the administration and customization of an intake form to support an ADRC/NWD (No Wrong Door) in the system. The intake form can be found online at: http://dhhs.ne.gov/medicaid/Aging/Documents/I_R%20and%20OC%20Intake.doc	X			
	Bidder's Response: VisualVault offers a no wrong door approach. A user who logs in will simply look in the forms list, find this and fill it in and submit. Workflow would auto route it based on the document classification. The caregiver management assessment can also be placed on the Department's website, downloaded, completed and either saved and submitted via an email or printed and mailed in. An individual can also complete the form and bring it to a local office.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
ASMT-13	Describe how the system accommodates InterRAI Assessment Instruments.	X			
	Bidder's Response: The InterRAI assessment instrument is a large form. VisualVault could use our iForms to create this tool to enable the state to gain all the benefits from working directly within the Elders First platform if the form is allowed to be copied. If not, the Elders First platform can integrate with the company's data collection form is that is permissible. VisualVault assumes the iForm would contain an estimated 600 fields.				
ASMT-14	Describe how the system accommodates the Supports Intensity Scale (SIS).	X			
	Bidder's Response: We would use the iForm template builder to create the SIS scale and work directly within the Elders First platform. This 12 page interview tool is estimated to have approximately 80 fields. Once the scale is configured in our iForm, NE gains all the benefits of working directly within the Elders First Platform as well as the online, offline capability.				

d. Usability

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
USE-1	The system must have copy/paste functionality.	X			
	Bidder's Response: Standard functionality				
USE-2	The system must be able to print, display, or export any information gathered in the client record, related to service usage, on a form and/or in a report.	X			
	Bidder's Response: Standard functionality				
USE-3	The system date must have 4 digit years.	X			
	Bidder's Response: Standard functionality				
USE-4	The system must have task and date reminder tracking.	X			
	Bidder's Response: Standard functionality using VisualVAult business rules.				
USE-5	Describe the system's customizable alerts. Describe how users are able to set alerts for activities like follow ups and next visits.	X			
	Bidder's Response: Core to VisualVault is the ability to set alert triggers based on many conditions. Data, time, month, annual, are examples of triggers that can be configured for the user community. The platform will be setup with the requested triggers and then added to, changed, or deleted by the system admin.				
USE-6	Describe the system's customizable workflows. For example, how a user would select, review, and document checked case files, service authorizations, service entries, and client demographics.	X			
	Bidder's Response: Customizable workflows through configuration is standard functionality. Using NE's example, a staff person would log into VisualVault. Their dashboard would appear and a list of "work" is presented. The list can be prioritized based on the users criteria. The user clicks on the item they want to open. The form or document opens for review. Comments can be attached, additional routing can be selected, approval or denial can be determined and the status represented as such. A link on the form can be clicked and view the GPS location of the address. Service listings can be viewed and selected as well. Across USE-1 through USE-13 requirements, we have assumed automation of two additional processes with three iForms averaging 50 data fields each. This automation includes the supporting workflow configuration, task notification, validation scripts, queries, and reporting.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
USE-7	Describe how the system supports cross-module workflows. For example, client eligibility for a funding source may be determined in one module by a separate state agency, and the client then referred to the AAA for services.	X			
	Bidder's Response: The system interfaces will capture the necessary information to meet this eligibility requirement.				
USE-8	Describe client portal products or options that are currently available. A client portal should be accessible by the client, or any person in their support network (caregiver, family member, neighbor, or friend). Describe security and access among public users.	X			
	Bidder's Response: A client portal will be available for the occasional user. However, this is where the Elders First model is superior to the traditional approach. The question to be answered is why are blind portals used for "external" user use? The answer is because to purchase enough software licenses to allow clients, caregivers, family members, etc. to work within the system has been too expensive. So email attachments and portals have been the workaround. VisualVault's Community Licensing transforms the old paradigm by licensing by the program area and supporting business processes to deliver The Aging Management Information System (NAMIS). Those involved in this program are able to have a license and therefore work directly within the system reducing the need to use the 1980s portal approach. True collaboration, self-service, accuracy of submittal and responses are a few of the benefits from working within the system. Instead of worrying about the 150-250 required licenses and costs, NE can focus on how to reengineer the processes to take advantage of this new paradigm and the positive affect on all stakeholders. VisualVault is prepared to discuss how Community Licensing will affect all aspects of the program.				
USE-9	Describe service provider portal products or options that are currently available.	X			
	Bidder's Response: Community Licensing will provide access to the Elders First platform. Providers simply log in and perform all work directly in the system. This innovative approach provides complete governance over every "transaction" with a complete audit trail of every action. In addition, the Elders First platform is a No-Wrong-Door platform that enables casual or one time users to use a portal to find required information and documentation. Experience indicates all service providers prefer to work within the system.				
USE-10	Describe the system's public service directory. Describe management and reporting options for information and referral component. Include website hits, validation, tracing incoming links, and comparison metrics.	X			
	Bidder's Response: We determine this based upon requirements gathering. VisualVault is an application development platform, with integrated content management, document repository, workflow, report design, screen design, analytics, and sophisticated web form design tool. Using the platform features we configure a case management and data management solution.				
USE-11	Describe how the system manages Rural/Non-Rural designations.	X			

	Bidder's Response: Rural/Non-rural designations would be identified on the iForm case file cover form. Several ways to identify this with a box to select, or drop down list to select are two options.				
USE-12	Describe how an AAA user would use the system to review a senior center's daily congregate meal entry for quality assurance purposes.	X			
	Bidder's Response: A user will have their own security and profile within the VisualVault system enabling a custom dashboard, workflow, and view of information. This AAA user will use the system to view their work queue of cases they need to review for quality assurance purposes. They will be able to see the senior center's daily congregate meal entries for the desired period of time. They will be able to compare this information to other similar centers and to the state standards to verify compliance with policy and regulations.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
USE-13	Describe automatic data capture technology capabilities such as bar coding.	X			
	Bidder's Response: At the core of the VisualVault solution is a suite of enterprise content management services. Bar code use is core to the ECM capability and can be incorporated on any iForm to help auto classify the document(s).				

e. Fiscal

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
FIS-1	Describe how the system tracks multiple funding sources for services, including Non-OAA funding sources. A client's meals may be originally paid for by one funding source, but then receive back-dated payment from another funding source. Describe how the software system would handle this scenario.	X			
	Bidder's Response: Funding sources is a configured field on iForms. Any funding source field can be designated as a "Non-OAA source by selecting the box next to it stating it is NOT an OOA source.				
FIS-2	Describe how the system tracks client funding across AAAs when the client record is moved from one AAA to another.	X			
	Bidder's Response: iForms are configured to capture funding elements.				
FIS-3	Describe how the system provides reconciliation, tracking and validating options for funding sources between the AAA and SUA.	X			
	Bidder's Response: iForms will be used to classify AAA and SUA users. Funding sources will be configured using iForms. Reconciliation fundings is done by the classification. Tracking is completed the same way. Validating funding sources is done with business rules within iForms and workflow.				
FIS-4	Describe how multiple fiscal years are tracked in the system.	X			
	Bidder's Response: The Elders First platform has core Enterprise Content Management suite functionality. All data and content is recorded as it is inputted. Date and times are auto linked to each action and activity and can be used to filter an unlimited number of fiscal years.				
FIS-5	Describe how the system provides FFR 425 reports.	X			
	Bidder's Response: A iForm will be created as the example below to create and populate the FFR 425 report.				

FEDERAL FINANCIAL REPORT
(Follow form instructions)

1. Federal Agency and Organizational Element to Which Report is Submitted	2. Federal Grant or Other Identifying Number Assigned by Federal Agency (To report multiple grants, use FFR Attachment)	Page 1 of pages
3. Recipient Organization (Name and complete address including Zip code)		
4a. DUNS Number / 4b. EIN	5. Recipient Account Number or Identifying Number (To report multiple grants, use FFR Attachment)	6. Report Type: ☐ Quarterly ☐ Semi-Annual ☐ Annual ☐ Final / 7. Basis of Accounting: ☐ Cash ☐ Accrual
8. Project/Grant Period (Month, Day, Year) From	To	9. Reporting Period End Date (Month, Day, Year)

10. Transactions	Cumulative
(Use lines a-c for single or combined multiple grant reporting)	
Federal Cash (To report multiple grants separately, also use FFR Attachment):	
a. Cash Receipts	
b. Cash Disbursements	
c. Cash on Hand (line a minus b)	
(Use lines d-o for single grant reporting)	
Federal Expenditures and Unobligated Balance:	

FIS-6	Describe how the system allows staff to track time per program and/or client, and bill for time within the system.	X			
	Bidder's Response: The Elders First platform auto tracks all actions and activities performed within the system. iForms and workflows can be used to start/stop the timer. The recorded time is auto linked to the activity being performed and is recorded for billing and reporting requirements.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
FIS-7	Describe how the system tracks received anonymous contributions by service. For example, how are Transportation service contributions kept separate from Congregate Meal contributions, and not tied to a client record?	X			
	Bidder's Response: The "type" of contribution could be a drop down field on the Contribution iForm. The staff person simply selects the appropriate contribution type and the classification is established. Contributions can be linked to a client record or anonymous contributions can be designated their own record type.				
FIS-8	Describe how indirect costs of services are tracked in the system.	X			
	Bidder's Response: We determine this based upon requirements gathering. VisualVault is an application development platform, with integrated content management, document repository, workflow, report design, screen design, analytics, and sophisticated web form design tool. Using the platform features we configure a case management and data management solution.				
FIS-9	Describe how direct costs of services are tracked in the system. Include costs that are not tied to a client.	X			
	Bidder's Response: We determine this based upon requirements gathering. VisualVault is an application development platform, with integrated content management, document repository, workflow, report design, screen design, analytics, and sophisticated web form design tool. Using the platform features we configure a case management and data management solution.				

f. Reporting

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
REP-1	List state(s) that have utilized the system for federal NAPIS reports for at least two federal fiscal years. Bidders that do not meet this qualification will not be considered.	C			
	Bidder's Response: VisualVault understands what is required for provide NAPIS reports and is fully capable of providing this report along with all other reporting requirements. We have assumed an interface with the Mediware system which typically produces this type of federal reporting.				
REP-2	The system must be able to support the federal NAPIS reporting. The State Program Report (SPR) requirements are expected to change by October 2019. Describe the bidders plan for these changes. https://acl.gov/news-and-events/announcements/older-americans-act-oaa-state-program-performance-report-spr-redesign	X			
	Bidder's Response: The NAPIS reporting will be developed as another reporting requirement within the solution as delivered. We have assumed 40 hours of developer time to meet this requirement. We will work with you to understand our needs in this area.				
REP-3	The system must be able to report on client demographic, service usage, units of service by service provider. List all standard reports included with the system.	X			
	Bidder's Response: VisualVault was originally a compliance tool designed to monitor and track all actions and activities occurring within the platform. Providing reports on demographics, service usage, units of service by service provider is core functionality by leveraging business rules to determine what data points being collected are required and then to setup the reporting format and timing. VisualVault customizes all reports for each client.				
REP-4	Describe how the system creates mailing lists based off of client demographics or service activity.	X			
	Bidder's Response: Creating mailing lists based on zip codes, counties, etc. is standard functionality. VisualVault identifies which field(s) in the data base is to be used to filter the list. The filter is applied and the list is generated. Same approach for service activity. Business rules are used to filter service definitions and the resulting list is created and then is output in the standard mailing format.				
REP-5	Describe dashboarding capabilities in the system, such as graphs, dashboards, cross fiscal year reporting, year to date, and year to year comparisons.	X			
	Bidder's Response: VisualVault's user interface is a dashboard. NE will determine what data is to be presented on the dashboard for each user group. Data is then presented based on the graphs and lists NE chooses to use. Dashboard views are configurable. Any data can be presented via the dashboard that resides within VisualVault or other 3rd party applications that the system is integrated with.				
REP-6	Describe the system's ability to create ad-hoc reports. Include specific user roles and licensing that may be required.	X			
	Bidder's Response: VisualVault's report functionality enable clients to create ad hoc reports on demand. This is core functionality.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
REP-7	Describe how the system would provide a county summary report that details services and client information for a given time period.	X			
	Bidder's Response: The Elders First platform records all actions and activities and maintains the data. Therefore, county data involving services during any data range is an easy report. The same data can be continually updated and presented in real time on the user's dashboard.				
REP-8	Describe the system's ability to generate reports for federal Congressional districts. Describe how districts realignment is managed.	X			
	Bidder's Response: The Elders First platform records all actions and activities and maintains the data. Federal Congressional districts will be identified when we configure the iForm that collects the first data. Filters will be applied to select Federal district data to be reported. The iForm will be configured to have a field that expands when the district changes based on business rules. The new district information is entered and the new data determines what is reported. This can be changed multiple times.				
REP-9	Describe the system's ability to generate reports for state legislative districts. Describe how districts realignment is managed.	X			
	Bidder's Response: The Elders First platform records all actions and activities and maintains the data. Same answer as above but the updateable field will be state legislative districts.				
REP-10	Describe the system's ability to generate Explanation of Benefits (EOB) reports that are personalized based on a client's assessment results and demographic data.	X			
	Bidder's Response: EOB reports are personalized by auto populating the meta data and demographic data from the client's iForm cover sheet. This can be done individually or in batch mode.				
REP-11	The system must be able to generate contribution request letters to enable program cost sharing.	X			
	Bidder's Response: A business rule is used to filter users to create the list of recipients. The list can be one single recipient or multiple. Once reviewed, the system prints the letters.				
REP-12	Describe the system's forecasting capabilities for service units and cost based off of previously entered data.	X			
	Bidder's Response: The Elder First platform offers substantial data analytics to run scenarios for forecasting and costs.				
REP-13	The system must be able to export data in reports. Describe file types that can be exported.	X			
	Bidder's Response: Standard functionality.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
REP-14	The system must be able to provide an audit log or snapshot of services provided, as entered on a specific date.	X			
	Bidder's Response: VisualVault tracks every activity and action in the system. All data collected from the monitoring is available to generate any audit log or snapshot of services. This can be done in real-time and presented to the user's dashboard or in report format.				
REP-15	Describe how the system tracks unpaid client balances for non-OAA services.	X			
	Bidder's Response: A business rule is used to run a routine every day that checks the iForm balance field. Client balance fields that do not equal $0 (zero) after X number of days will be identified and a unpaid balance report will be generated and loaded in the appropriate staff inboxes for review and action. A letter and or email can be generated and sent to the client. .				

g. Volunteer management

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
VOL-1	Describe the system's volunteer management capabilities.	X			
	Bidder's Response: The system is able to establish any number of user profiles and customize the access to information for that individual or class of users. The volunteers would be able to enter their information to the state system and have a limited view into the content the state deems appropriate. The system is able to provide dashboard information and reporting to the management team responsible for coordinating volunteer groups and activities. We have assumed the configuration of a custom iForm with approximately 50 fields to capture volunteer information, a custom workflow, configured validation, query and reporting capability to support volunteer management.				
VOL-2	Describe how the system differentiates between stipend volunteers like the Federal Senior Companion, Foster Grandparents programs, and unpaid volunteers.	X			
	Bidder's Response: The system is able to separate categories of users and/or workers according to different funding sources, their work assignment profile, and a host of other variables that allow Nebraska to separately manage stipend volunteers from unpaid volunteers. The system can demonstrate the value each of these groups is providing to the citizens and enable case management of all the support functions for these groups. We can interface with payment process applications as needed to support the stipend volunteer programs.				

h. Provider Information

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PRV-1	The system must be able to manage service provider information, including services, population served, address, name, email, phone, and website.	X			
	Bidder's Response: VisualVault provides the solution for FL's Department of Children and Families, Substance Abuse and Mental Health. A major portion of the system manages the 2,000+ service providers. All service provider data is collected using the iForm cover sheet to their file and maintained within the repository. This is core functionality. The platform also provides the assessment forms, creates the deficiency reports, the corrective action plans (CAPS) licensing, renewals, and more.				
PRV-2	The system must be able to manage multiple service contracts/rates for a single provider.	X			
	Bidder's Response: Standard functionality using iForms and business rules. We have assumed the use of an iForm with approximately 50 fields, a workflow configuration, validation script, and supporting reporting to manage service provider information to address PRV-1 through PRV-5 requirements.				
PRV-3	Describe how the State can customize the system with ad-hoc field creation for Service Providers, including contract/rate management.	X			
	Bidder's Response: Standard functionality using our iForm and the iForm template builder. The State will be able to use the drag and drop capability to make changes to customize the fields for Service Providers.				
PRV-4	The system must provide service provider search functions.	X			
	Bidder's Response: Core functionality is our Enterprise Content Management suite of services. Robust search is core to ECM functionality. Service Providers will log in and conduct searches directly within the system at any time.				
PRV-5	The system must be able to edit a service provider for multiple clients at once. For example, Company X provides Emergency Response Systems to fifty clients in January. The contracted service provider is changed to Company Y in February. Describe a bulk client move from Company X to Company Y.	X			
	Bidder's Response: We determine this based upon requirements gathering. VisualVault is an application development platform, with integrated content management, document repository, workflow, report design, screen design, analytics, and sophisticated web form design tool. Using the platform features we configure a case management and data management solution.				

i. Operations

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
OPR-1	Describe how the system will support Area Plan management. Describe how AAAs could upload and add data to a template. Describe how the SUA could review, provide remarks, return to AAA, or approve Area Plans and their updates. Current Area Plans are located at: http://dhhs.ne.gov/medicaid/Aging/Pages/Financial-Program-Data.aspx	X			
	Bidder's Response: The Area Plans can be another iForm in the VisualVault system. Once this template is created, the plans can be loaded into the system and all the power of the VisualVault platform is available to query, report, and manage this information. We will work with you to determine whether prior year plans need to be loaded into the system. We have assumed they do not exist in an automated fashion today. We have assumed the automation of the Area Plans will be supported via an iForm with approximately 50 fields to provide a way to load the information into the system. We have assumed a workflow with validation and queries to use this information.				
OPR-2	Describe how the system supports local service creation. Describe how the AAA creates and submits a new service for the SUA to review and approve.	X			
	Bidder's Response: This is an example of the flexibility of the VisualVault platform. Creation of a new service, approval of that service, and ultimately tracking of that service becomes a new process in our system. This allows the state to track information from start to finish and use the workflow management capabilities to support the needs of a new service creation.				
OPR-3	Describe how the system supports AAA Care Management Re-Certification. Describe how AAAs could upload and/or add data to a template. The SUA could review, provide remarks, return to AAA, or approve Care Management Re-Certifications. Guidance on FY 2019 Recertification can be found here: http://dhhs.ne.gov/medicaid/Aging/Documents/SUA-18-PI-04%20Care%20Management%20Recertification%20FY%2019.pdf	X			
	Bidder's Response: VisualVault supports many licensing applications and re-certification is a common function for many of our clients. The VisualVault platform is configured to meet the steps in your AAA Care Management re-certification process with the supporting iForms to upload and/or add data. The SUA can review the re-certification application, provide remarks, return to AAA, or approve Care Management Re-Certifications. We have assumed a separate iForm will be required to support re-certification along with a separate workflow, validation rules, queries and reports. We assumed the iForm will have approximately 50 fields included in it.				
OPR-4	Describe how the system supports the Direct Service Waiver application process. Describe how the AAAs upload and/or add data to a template. Describe how the SUA could review, provide remarks, return to AAA, or approve Direct Service Waivers. The Direct Services Waiver forms and process are located online at: http://dhhs.ne.gov/medicaid/Aging/Documents/Direct%20Service%20Waivers%20Forms%20+%20Procedure.doc	X			
	Bidder's Response: The VisualVault platform supports the Direct Service Waiver application process via our iForms and built-in platform for Nebraska processes. This allows automation of the existing application process and the full capability of the platform to support queries, reporting, dashboards, and workflow management.				

	We have assumed a separate iForm with approximately 50 fields in it will be required to support the Direct Service Waiver process. The iForm will be supported by a configured workflow, validation script, queries, and reporting to meet this requirement.				
OPR-5	Describe the system's document library capabilities such as report and letter templates.	X			
	Bidder's Response: A document library containing report and letter templates is standard out of the box functionality. Content can be saved and pulled to populate outbound communication.				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
OPR-6	Describe how the system supports SUA monitoring questions, and allows AAA program staff to record responses. Current monitoring tools are located at: http://dhhs.ne.gov/medicaid/Aging/Pages/Monitoring-Tools.aspx	X			
	Bidder's Response: The VisualVault platform can automate each of the monitoring checklists to allow AAA program staff to record responses, compare information, track trends, and follow-up on issues using the workflow management process support tools. We have assumed one iForm with approximately 50 fields will be required to automate the monitoring tool. This will be accompanied by the supporting workflow configuration, validation rules, queries and reporting.				
OPR-7	Describe how the system supports creating, editing, and storing SUA monitoring letters to AAAs. A draft monitoring letter is located online at: http://dhhs.ne.gov/medicaid/Aging/Documents/FY18%20Monitoring%20Letter%20DRAFT.doc	X			
	Bidder's Response: The VisualVault platform can easily automate the creation, editing, and storing of SUA monitoring letters to AAAs. This process can be incorporated into the overall workflow management process and the power of the platform supports all the tracking activities associated with the process.				

j. Testing / Training

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TET-1	Describe any user groups of existing clients, conferences, and webinars. Include their frequency.			X	
	Bidder's Response: No user group of existing clients yet but we are looking at that for 2020. We will have two webinars in 2019.				
TET-2	Describe Bidder help desk services available to the state, area agencies on aging, and other providers at no additional cost to the State. Include hours of operation, location of the call center, response time statistics, how calls are answered, triaged, and any functional limitations.	X			

Bidder's Response: VisualVault provides help desk based on our standard SLA that is included in our response.

1. **Standard On Call Support.**
   1.1. The Principal Period of Support ("PPS") is a ten (10) hour contiguous daily time period between the hours of 8:00 AM and 5:00 PM, Eastern US local time, Monday through Friday, excluding VisualVault's published holidays or holidays as observed locally by VisualVault. All Support subsequently added will have the same PPS.

2. **Severity Levels.**

Based on communications between Subscriber and VisualVault, the parties shall determine, in accordance with the following table, the "Severity Level" of each issue.

Severity Level	Definition
1	**An issue that causes the Software to crash or be unavailable for use and which has no acceptable work-around.**
2	**An issue that affects multiple users of the Software and prevents effective use of an essential feature or essential features of the Software, but which does not cause the Software to be unavailable for use in whole.**
3	**An issue that affects productivity or ease of use of the Software and for which there is typically a work around.**

4	**An issue that does not materially affect Subscriber's (or any Subscriber Customer's) ability to use the Software (e.g., user interface inconveniences).**

Severity Level	VisualVault Responsibilities	Client Responsibilities
1	Acknowledge and begin addressing immediately. VV's Client support and production support teams will work continuously until fixed, 24x7 if not resolved by the close of the business day. Such 24x7 effort to commence first business day after determination of severity. Target resolution time is four (4) hours.	Call at time of discovering issue (email not acceptable for Severity 1). Be available to answer questions, provide information, and receive and install code fix immediately, 24x7 if not resolved by the close of the business day.
2	Acknowledge and begin addressing promptly. VisualVault's Client support and production support teams will work continuously within normal business hours until resolved. Target resolution time is 24 hours.	Be available to answer questions, provide information within four (4) hours of request. Install/test fix providing feedback.
3	Acknowledge within one business day. Issue will be	Provide information and answer questions within one (1) business day.

			scheduled to be addressed, based on the priority set by Client and VV. Target resolution time is seven (7) days.		
		4	Acknowledge within one business day. Issue will be addressed when possible, based on the priority set by Subscriber and VisualVault.	Provide information and answer questions within three business days.	

k. Data / Data Warehouse

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DAT-1	The State must retain all rights to data. At the end of contract, the Bidder must provide all data in a format specified by the state, for use in another software system. Provide in draft project plan.	X			
	Bidder's Response: VisualVault agrees with this requirement and will comply.				
DAT-2	Bidder must be able to convert current Nebraska Aging Management Information System (NAMIS) client demographic data into proposed system. See Appendix A-1.	X			
	Bidder's Response: VisualVault's implantation partner ProCom Consulting provides unparalleled expertise and experience in data migration. We will provide a detailed description of ProCom's history and capability. We have included the effort to plan the conversion, automate the data conversion, test it, and provide control reports to verify the completeness and accuracy of the work prior to system go-live We have assumed this data is clean and will not require manual correction prior to upload to the new platform.				
DAT-3	Bidder must be able to convert current Aging and Disability Resource Center client demographic data into the proposed system. See Appendix A-2	X			
	Bidder's Response: VisualVault's implantation partner ProCom Consulting provides unparalleled expertise and experience in data migration. We will provide a detailed description of ProCom's history and capability. We have included the effort to plan the migration of this data from the excel extract to the new platform, test the process, and verify the results.				
DAT-4	Describe how the system could interface with State data warehouse/s. Describe the frequency of data refreshes. Describe the options for the download, such as Bidder software, or an import /conversion to an existing state data warehouse. Include information on master data, which refers to data elements that should be shared across the systems, data elements such as Social Security Number, address and last name.	X			
	Bidder's Response: Standard API and or micro-services enable the Elders First Platform to integrate with any open application. A DHHS business rule will determine the frequency of data refreshes. The number is client determined. We have assumed 160 hours of developer time to build an interface with the State data warehouse to your specifications. During the discovery and requirements phase, we will work with you to determine the way the State wants this interface to work. We are flexible on the options for downloading and/or an import process depending on your detailed needs.				
DAT-5	Describe how the system can interface with Mediware's SAMS product being used by two AAAs.	X			

	Bidder's Response: We have assumed 160 hours of developer time to build an interface with the Mediware SAMS product to provide importing/exporting of data pursuant to the State's needs. During the discovery and requirements phase, we will work with you to determine the details of how this interface should work and implement the interface using our microservices feature.

DAT-6	Describe the system's data edits and validation processes; including soft (warning, but accepted upon user approval); and hard (correction required to record). Describe available customizations. iForms are used to capture data. If a field is "edited" or updated, the new information is saved as a revision to the original to maintain the chain of custody. Any filed can have a business rule applied to validate an verify data. If flawed data is entered, a notification will flash alerting the person of the error and directing them to change their entry. A business rule can be used to not allow non validated or flawed data to be saved. iForms are completely customizable using the iForm drag and drop template.	X			
	Bidder's Response:				
DAT-7	The system would allow the State to manage data entry time limits. For example, entry changes after 30 days should require State personnel approval. Describe the workflow creation process to address this need.	X			
	Bidder's Response: Time triggers within workflows and iForms can be used to manage data entry time frames. Each document is classified by the doc type or meta data. The business rule associated with the timeframe and iForm is typically automatically set when it is routed from one stop to the next or when it is saved to the repository. Alerts can be sent based on the number of days ahead of the time elapsing to warn staff of an impending event. Once an entry requirement passes the 30 day period, the business rule behind the workflow will auto route it to state staff for approval.				

I. Security

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SCT-1	The system must be able to accommodate different user roles depending on job.	X			
	Bidder's Response: VisualVault standard functionality. VisualVault has no limit on the number of user roles that can be created.				
SCT-2	Describe how the system is able to securely store, edit, and save client assessments offline (case managers will not always have access to the internet during assessments).	X			
	Bidder's Response: iForms are used to create the assessment form. iForms work online and offline. Internet connectivity is not required to complete the form. The Assessor will complete the form and save it to their local drive. When they return to an area where they have connectivity, VisualVault will synchronize and auto upload the assessment.				
SCT-3	Describe online / offline upload / download capabilities, include what portable devices are available for the synchronization process.	X			
	Bidder's Response: VisualVault iForms are designed to function online and offline. Assessments and other iForms are saved to the local device and when reconnected to the internet, synch to VisualVault and based on the document classification, will be routed to the right person, or saved to the repository. VisualVault uploads and downloads to all major devices. VisualVault's smart phone capability also provides a range of functionality associated with today's smart phone applications. VisualVault's remote capabilities combined with Community Licensing that engages the entire community of users, will enable NE to provide a new level of collaboration with those you serve and those who provide the services.				

CLI -5 GRAPHIC

Attachment C | VisualVault Response
Optional Ombudsman Business Requirements Traceability Matrix

Request for Proposal Number 5948 Z1

How to complete the Optional Ombudsman Business Requirement Traceability Matrix:

Column Description	Bidder Responsibility
Req #	The unique identifier for the requirement as assigned by DHHS, followed by the specific requirement number. This column is dictated by this RFP and must not be modified by the bidder.
Requirement	The statement of the requirement to which the bidder must respond. This column is dictated by the RFP and must not be modified by the bidder.
(1) Comply	The bidder should insert an "X" if the bidder's proposed solution complies with the requirement. The bidder should leave blank if the bidder's proposed solution does not comply with the requirement. If left blank, the bidder must also address the following: • Capability does not currently exist in the proposed system, but is planned in the near future (within four months from the date of submission of the bid) • Capability not available, is not planned, or requires extensive source-code design and customization to be considered part of the bidder's standard capability • Requires an extensive integration effort of more than 500 hours
(a) Core	The bidder should insert an "X" if the requirement is met by existing capabilities of the core system or with minor modifications to existing functionality.
(b) Custom	The bidder should insert an "X" if the bidder proposes to custom develop the capability to meet this requirement. Indicate "custom" for those features that require substantial or "from the ground up" development efforts.
(c) 3rd Party	The bidder should insert an "X" if the bidder proposed to meet this requirement using a 3rd party component or product (e.g., a COTS vendor, or other 3rd party). The bidder must describe the product, including product name, its functionality and benefits in their response.

1, Unique to the State Long-Term Care Ombudsman Program (LTCOP)

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
1.	Describe the long term care ombudsman capabilities that can track all required fields for National Ombudsman Report System (NORS).	X			
	Bidder's Response: This is a core function of VisualVault. The advantage of the VisualVault platform is our ability to use iForms to collect data either manually or downloaded to the form. Business rules filter data. And, VisualVault can export data in any standard format. Therefore, collecting, formatting, and outputting data for NORS use will all be automated and run on the scheduled basis with no manual intervention required other than to review.				
2.	Describe how the system accommodates different user roles.	X			
	Bidder's Response: VisualVault defines roles within the system. Once rolls are defined, we then determine the functions required for that roll and assign them to the group. This simple design enables system administrators to easily change and make new user roles.				
3.	Describe how volunteer Ombudsman are managed in the system. Volunteers will not need access to system.	X			
	Bidder's Response: The VisualVault Team will create a roll titled "Volunteer Ombudsman". We then assign functions to the roll. VisualVault assumes Ombudsman will complete a "registration" iForm to provide the appropriate metadata. When they sign and submit the form, a digital file will be created for them. Support documents can be uploaded to the file by dragging and dropping electronic docs from their computer. A list of volunteer Ombudsman can be presented on the staff's dashboard, or a search will return one or multiple files. All other management activities occur by simply searching for the file and opening it.				
4.	Describe how nursing facilities and assisted living facilities are managed in the system.	X			
	Bidder's Response: The VisualVault Team will create rolls for all groups. We then assign all the functions to the rolls. Licensing and renewals are often part of the onboarding process. A "registration" iForm will be completed to provide the appropriate metadata. When they sign and submit the form, a digital file will be created for them. Support documents can be uploaded to the file by drag and dropping electronic docs from their computer. A list of volunteer Ombudsman can be presented on the staff's dashboard or a search will return one or multiple files. All other management activities occur by simply searching for the file and opening it.				
5.	Describe how the system creates and tracks corrective action plans.	X			
	Bidder's Response: The VisualVault solution implemented in another state transformed the assessment/deficiency/corrective action plan (CAP) process for our client. The state was open to reengineering the process, and we worked together to develop the best solution. Within the client's assessment form, we created note fields and a library of deficiencies. The inspector (the state's term) selects the deficiency from the library, and the note fields populates. When the deficiency note is created, an additional note field opens for the Provider to write their CAP information. Since the provider, inspector, and other state staff are all working directly within the system, the entire exchange of work is recorded for audit and improved governance. Notifications that the deficiency report				

	has arrived, and they need to log in and review the findings is sent. All work occurs in real-time inside VisualVault. The corrective action plan (CAP) is created as they reply to each deficiency. When they have completed the CAP, they sign it using VisualVault's eSignature and submit. A notification is sent to the inspector. They open the notification from their inbox, review, and either approve or deny. Once approved, the entire documentation is filed and linked to the provider. Tracking by anyone involved in the process is a self-serve task because they simply look at what step it is in the workflow and who is responsible for that step.				
6.	Describe how the system documents LTCOP cases, complaints, corrective action plans, and follow up.	X			
	Bidder's Response: VisualVault documents information using iForms configured for the required process. The ability to configure iForms to include all required questions, plus note fields will enable Ombudsman and all others involved in a complaint, case, CAP, etc. to have a single view and capture tool to assure accuracy. VisualVault has provided several images of iForms in our response to illustrate the dynamic capability these forms have, as well as the ability to be changed and expanded as requirements evolve. (A high-level overview of the process using a complaint follows) • A complaint iForm is used to capture the initial information • When it is submitted, workflow routes it to the appropriate person(s) based on document classification and other metadata • A triage of the information is performed, and an initial determination is made as to the validity of the complaint • If it is decided the compliant if valid, the Elders First platform auto generates a case number and assigns the case to the appropriate case worker • At this point, the complaint is now an official case • The case file is automatically set up • The case worker uses calendaring to set the appointment • The assessment is performed using the assessment iForm that is linked to the original complaint form • The findings can be distributed to other staff and management for review using workflow • The determination is made, recorded on the form, and notifications and other correspondence is sent to all stakeholders • Each action taken has been recorded by VisualVault • Who did what, the time, the action taken is all recorded and can be viewed on a dashboard or within a report • Therefore, The Elders First Platform is continually documenting all actions and activities and the data can be used to provide complete transparency because all actions are occurring within the system				

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
7.	Describe how the system tracks LTCOP activities, consultations, and trainings.	X			
	Bidder's Response: Much of what we stated in the question #6, above relates to this requirement. All activities are recorded in VisualVault. Consultations can be recorded using a configured iForm to record the discussion. This information is linked to the case, file, or event based on metadata, document classification and or other unique ID type data fields. Business rules can be used to set triggers for reminders, required actions, etc. Each of these are tracked and recorded as well. Dashboards and reports can present the information as required.				
8.	Describe how the system data verification activities are managed at the local and state level.	X			
	Bidder's Response: All data being entered using an iForm can be validated as it is entered using business rules behind each field. If the data is determined valid, the Elders First platform can query the VisualVault database or other 3rd party databases to validate the information. Typically, this is an automated function based on doc type and data field within the document.				
9.	Describe information regarding the database, collection of required data elements, how required fields are flagged, and how data is verified prior to submission and certification at the federal level.	X			
	Bidder's Response: Elders First has a robust repository and uses iForms to collect data for entry. Business rules are used on required fields that flag the individual immediately and offers a pop up to give help hints. Business rules also are used to validate information as it is entered. The Elders First platform can query the VisualVault database or other 3rd party databases to validate the information. Typically, this is an automated function based on doc type and data field within the iForm.				
10.	Bidder must be able to convert Federal Fiscal Year 2017, 2018 and 2019 Ombudsman database data into proposed system. Provide a conversion plan.	X			
	Bidder's Response: VisualVault's national implementation partner, ProCom Consulting, is a nationally recognized leader in database conversion and migration. Please see their resume in the VisualVault response to understand the depth of expertise and experience they bring to this important part of the project.				

Attachment D
Technical Requirements Traceability Matrix

VisualVault Response
Request for Proposal Number 5948 Z1

Bidders are instructed to complete a Technical Requirements Traceability Matrix for Aging Services software replacement. Bidders are required to describe in detail how their proposed solution meets the conformance specification outlined within each Technical Requirement.

The traceability matrix is used to document and track the project requirements from the proposal through testing to verify that the requirement has been completely fulfilled. The contractor will be responsible for maintaining the contract set of Baseline Requirements. The traceability matrix will form one of the key artifacts required for testing and validation that each requirement has been complied with (i.e., 100% fulfilled).

The traceability matrix should indicate how the bidder intends to comply with the requirement and the effort required to achieve that compliance. It is not sufficient for the bidder to simply state that it intends to meet the requirements of the RFP. DHHS will consider any such response to the requirements in this RFP to be non-responsive and the bid may be rejected. The narrative should provide DHHS with sufficient information to differentiate the bidder's technical solution from other bidders' solutions.

The bidder must ensure that the original requirement identifier and requirement description are maintained in the traceability matrix as provided by DHHS. Failure to maintain these elements may render the bid non-responsive and result in for rejection of the bidder.

How to complete the traceability matrix:

Column Description	Bidder Responsibility
Req #	The unique identifier for the requirement as assigned by DHHS, followed by the specific requirement number. This column is dictated by this RFP and should not be modified by the bidder.
Requirement	The statement of the requirement to which the Bidder should respond. This column is dictated by the RFP and must not be modified by the Bidder.
(1) Comply	The Bidder should insert an "X" if the Bidder's proposed solution complies with the requirement. Describe in the response how the Bidder's proposed solution meets the requirement. The Bidder should leave blank if the Bidder's proposed solution does not comply with the requirement. If left blank, the Bidder should also address the following:

Column Description	Bidder Responsibility
	• Capability does not currently exist in the proposed system, but is planned in the near future (within the next few months) • Capability not available, is not planned, or requires extensive source-code design and customization to be considered part of the Bidder's standard capability • Requires an extensive integration effort of more than 500 hours
(a) Core	The bidder should insert an "X" if the requirement is met by existing capabilities of the core system or with minor modifications or configuration to existing functionality.
(b) Custom	The bidder should insert an "X" if the bidder proposes to custom develop the capability to meet this requirement. Describe and indicate "custom" for those features that require substantial or "from the ground up" development efforts.
(c) 3rd Party	The bidder should insert an "X" if the bidder proposed to meet this requirement using a 3rd party component or product (e.g., a COTS vendor, or other 3rd party). The bidder must describe the product, including product name, its functionality and benefits in their response.

TECHNICAL REQUIREMENTS

The following requirements describe what is needed to support DHHS technical project operations.

Each requirement is identified by the following first three characters:

TEC	General Technical Requirements
STN	Standards Requirements
ERR	Error Handling Requirements
DBM	Database/Data Management Requirements
BKP	Backup and System Recovery Requirements
SEC	Security Requirements
DOC	System and User Documentation
TRN	Training
PTT	Production, Test and Training Requirements
INT	Interfaces/Imports/Exports Requirements
PER	System Performance Requirements

General Technical Requirements

This section presents the overall technical requirements that apply to the software. Describe in the Response how the proposed solution meets the requirement.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TEC-1	Provide a description and diagram of the Bidder's proposed technical architecture. Include all database/web/networking hardware, software, tools, and information on where the solution is hosted.	X			
Response: Please see Attachment G - GRM VisualVault Network Architecture (redacted).pdf and Attachment D - GRM VisualVault Technical Summary.pdf					
TEC-2	If the Bidder's proposed solution requires any DHHS data to be stored off-site (including data "in the cloud") describe how the data is stored in federally compliant data centers residing within the continental United States of America and follows HIPAA standards.	X			
Response: VisualVault's cloud computing environment resides within four AWS availability zones. All data is encrypted in transit and at rest. VisualVault undergoes regular third party external vulnerability assessments, daily internal vulnerability scans. Third party assessments are conducted annually for SOC-1, SOC-2 (SSAE-18), and HIPPA HITECH.					
TEC-3	Describe how the solution is designed so that business rule parameters and code lookup tables can be easily updated without changing the overall application program logic.	X			
Response: The VisualVault platform is designed using SOA and microservices architecture combined with low code application development features. Multiple core product features enable business rule and application configuration without changing the overall application program logic. These application design features include: Web form designer with support for sophisticated drag and drop html form design, analytics dashboard designer, advanced report designer, ad-hoc report builder, portal screen builder, and microservices library.					

TEC-4	Describe the software licensing model of the solution, including any required third party licensing. Describe how the Bidder's maintains licensed software no more than two supported versions behind the latest release and updated with latest security patches	X			
Response: VisualVault Community Licensing offers a completely new and unique model that allows NE to have all program participants work directly within the system and benefit from the use. No other vendor offers this model and the associated benefits. All product features and modules are included in the annual subscription fee. Security patches are applied when needed. Minor software version upgrades are deployed quarterly when available. Major version updates are typically applied annually. A sandbox environment is updated in advance providing the opportunity for testing and approving major updates.					
TEC-5	Describe any impact to the solution when customizations are made for upgrades and maintenance processes. DHHS prefers to minimize downtime and impact to the users.	X			
Response: All customer use the same core product platform. Customizations and configurations are implemented using product features, microservices, and product API integrations.					
TEC-6	Describe how the proposed solution is scalable and flexible enough to accommodate any changes required by the State and/or federal statute, mandate, decision or policy.	X			
Response: Multiple core product features enable business rule and application configuration without changing the overall application program logic. These application design features include: Web form designer with support for sophisticated drag and drop html form design, analytics dashboard designer, advanced report designer, ad-hoc report builder, portal screen builder, and microservices library.					
TEC-7	Describe how the system stores objects such as pictures, documents, PDF files, etc. If an electronic document management system is part of the solution, provide a description of the proposed document system and how it is able to support multiple objects.	X			
Response: VisualVault includes a scalable document repository as part of the core platform. Any file type may be stored. File metadata is stored in databases and files are stored encrypted within AWS S3.					

TEC-8	Describe how the proposed solution is responsive to mobile technology and works with mobile devices such as smart phone or tablets.	X			
Response: VisualVault uses responsive design to accommodate mobile devices. Also included is an offline forms feature allowing form submissions from mobile devices without an Internet connection (synchronize data when connection is available).					
TEC-9	Describe what industry standard browsers are supported by the Bidder's solution.	X			
Response: All modern browsers including Chrome, Firefox, Edge, Safari, IE 11+					

Standards Requirements

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
STN-1	Describe how the Bidder's proposed solution complies with accessibility requirements described in the State of Nebraska accessibility requirements located at http://nitc.nebraska.gov/standards/2-101.html	X			
Response: VisualVault publishes a Voluntary Product Accessibility Template (VPAT). Please see Attachment A4 - VisualVault_Section 508 VPAT.pdf					
STN-2	Describe how the Bidder's proposed solution conforms to the sub-parts of Section 508 of the Americans with Disabilities Act (ADA), and any other appropriate State or federal disability legislation. Refer to http://www.ada.gov/508/.	X			
Response: VisualVault publishes a Voluntary Product Accessibility Template (VPAT). Please see Attachment A4 - VisualVault_Section 508 VPAT.pdf					
STN-3	Describe how the Bidder's proposed solution is consistent with all HIPAA and other statutory, regulatory and policy requirements as defined and adopted by DHHS. Refer to http://dhhs.ne.gov/Pages/fin_ist_policies.aspx for policies and standards.	X			
Response: All data encrypted in transit and at rest. Annual HIPAA-HITECH third party assessment. Please see Attachment A3 - GRM VisualVault 2018 Type 1 HIPAA Final Report.pdf					

Error Handling Requirements

The management of the system requires that all occurrences of errors be logged for review and that critical errors be accompanied by appropriate alerts. Authorized users need to be able to query and review the error log and configure the alerts.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
ERR-1	Describe the Bidder's proposed Error Handling functionality.	X			
Response: Centralized error handling with logs stored in a centralized log repository.					
ERR-2	Describe how the Bidder's proposed solution provides a comprehensive set of edits at the point of data entry to minimize data errors and provide immediate feedback in order for incorrect data to be corrected before further processing.	X			
Response: The primary feature set used for this is our intelligent forms combined with configurable business rules and data validation.					
ERR-3	Describe how the Bidder's proposed solution ensures all errors are written and categorized to an error log. Describe how the Bidder's proposed solution allows for a user to view, filter, sort, and search the error log.	X			
Response: Centralized error handling with logs stored in a centralized log repository. Log data can be accessed from the integrated report writer supporting filtering, sorting, or searching.					
ERR-4	Describe how the Bidder's proposed solution provides for the generation of standard and customizable error reports.	X			
Response: Centralized error handling with logs stored in a centralized log repository. Log data can be accessed from the integrated report writer supporting filtering, sorting, or searching.					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
ERR-5	Describe how the Bidder's proposed solution has the ability to suppress error messages based upon user-defined criteria.	X			
Response: Most error messages displayed after implementation are business process specific messages decided upon during the project discovery phase.					

Database/Data Management Requirements

DHHS requires the benefits inherent with a relational database management system (RDBMS). The accessibility, flexibility and maintainability achieved through normalized data structures are essential to achieving the business objectives outlined in this RFP.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DBM-1	Describe the Bidder's proposed Database architecture including the database software is supported by the proposed application.	X			
Response: VisualVault is a hosted (SaaS) solution using multiple database technologies including relational and non-SQL databases. An integrated report writer is included in the base product platform.					
DBM-2	Describe the Bidder's proposed Database Warehouse solution, if applicable.				X
Response: We do not include a Data Warehouse but can interface with an existing data warehouse.					
DBM-3	Describe how the Bidder's proposed solution is built upon an integrated data model, such as a Relational Database Management System (RDBMS), with referential integrity enforced. Describe the integrated data model.	X			
Response: VisualVault is a hosted (SaaS) solution using multiple database technologies including relational and non-SQL databases. With this type of homogenous database architecture referential integrity is enforced with the application layer.					
DBM-4	Describe how the Bidder's proposed solution maintains an automated history of all transactions, including, but not limited to: date and time of change, "before" and "after" data field contents, and operator identifier or source of the update.	X			
Response: VisualVault maintains transaction logs for users, documents, forms, and business objects. Intelligent forms are used as the basis for most end user interaction; these forms support field level change tracking and automatic revisioning of data.					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DBM-5	Describe the ability for the Bidder to convert data from the current systems utilized into the Bidder's proposed solution. Describe the technology used to complete the conversion.	X			

Response: Our data conversion approach is based both on VisualVault's successful track record as well as the expertise our teaming partner ProCom brings from large data migration projects within regulated environments where both the timing and accuracy of data migration is paramount. For example, since 1999 Frontier Communications has relied on ProCom to provide data migration to support post-merger integration and other major technology projects, with a total of more than 50 Billion data records and more than 1.5 Billion documents successfully migrated from multiple source systems. We have experience with a number of ETL tools but prefer to utilize Talend. We can work with ETL tools that you currently use if preferred.

Backup and System Recovery Requirements

DHHS requires the ability to create backup copies of the software and to restore and use those backup copies for the basic protection against system problems and data loss. This requirement refers to all application system files, data files, and database data files. The Bidder's proposed solution should provide a comprehensive and easily manageable backup and recovery process that is responsive to DHHS needs.

The Bidder's proposed solution should identify and implement a system recovery plan that ensures component failures do not disrupt services. The plan should be completed, implemented, and tested prior to system implementation.

The successful Bidder's solution should specify all needed hardware, software, and tools, and the plan should clearly define all roles, responsibilities, processes, and procedures. The solution should be sufficiently flexible to integrate with existing DHHS capabilities and accommodate future changes.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
BKP-1	Describe the Bidder's proposed Backup and System Recovery plan and readiness. Describe the Bidder's service level agreement on returning the solution to service from a backup. Describe the Bidder's proposed backup retention schedules – daily, weekly, monthly, quarterly, etc.	X			
Response: Please see Attachment L - GRM VisualVault Data Retention Backup and Restore (SOP-0009).pdf					
BKP-2	Describe the Bidder's proposed Disaster Recovery Plan. Describe the Bidder's service level agreement on returning the solution back to operational service.	X			
Response: Please see Attachment F - GRM VisualVault Disaster Recover and Business Continuity Plan (ISO-0015).pdf					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
BKP-3	Describe how backups of the Bidder's proposed solution are able to be scheduled without user intervention and without interruption to the system.	X			
Response: Fully automated backup process monitored by VisualVault operation staff.					
BKP-4	Describe how the Bidder's proposed solution provides information on their test and validation process for all of the backup requirements listed previously (BKP-1, BKP-2, and BKP-3).	X			
Response: We conduct periodic tests as well as an annual Disaster Recovery Plan test.					
BKP-5	If there is a backup failure or downtime, describe the Bidder's proposed method and timing of communication to DHHS.	X			
Response: VisualVault maintains a live system status page available at https://status.visualvault.com where customers may subscribe to downtime, scheduled maintenance, and other system status notification events.					

Security and Audit Requirements

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-1	Describe the Bidder's proposed security safeguards integrated into their application and how these safeguards address DHHS security. Refer to DHHS Information Technology (IT) Access Control Standard (DHHS-IT- 2018-001B) for specific requirements: http://dhhs.ne.gov/Pages/fin_ist_policies.aspx	X			
Response: • Formal security policies and procedures • Formal software development standards • All data encrypted in transit and at rest. • Annual third-party audits including: SOC-1, SOC-2 (SSAE-18), HIPAA HITECH • Employee training • Daily internal vulnerability scans • Period external third-party vulnerability scans • Single Sign On via SAML2 protocol (allows customer to use their SAML2 compliant identity provider to manage user accounts). This option also supports multi-factor authentication. • Centralized logging and log monitoring • Security best practices within cloud computing environment architecture (single purpose network segments, hardware based key management modules, etc.)				
SEC-2	Describe how the Bidder's proposed solution complies with Federal, State, and division-specific security requirements including but not limited to: • Health Insurance Portability and Accountability Act (HIPAA) of 1996 • Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 • Privacy Act of 1974 • 45 CFR Part 164 Security standards for PHI • Office of the National Coordinator's Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health information Refer to the Nebraska DHHS Information Systems and Technology Security Policies and Standards for more information (http://dhhs.ne.gov/Pages/fin_ist_policies.aspx).	X			

Response:

- BAA agreements
- Formal security policies and procedures
- Formal software development standards
- All data encrypted in transit and at rest.
- Annual third-party audits including: SOC-1, SOC-2 (SSAE-18), HIPAA HITECH
- Employee training
- Daily internal vulnerability scans
- Period external third-party vulnerability scans
- Single Sign On via SAML2 protocol (allows customer to use their SAML2 compliant identity provider to manage user accounts). This option also supports multi-factor authentication.
- Centralized logging and log monitoring

Security best practices within cloud computing environment architecture (single purpose network segments, hardware based key management modules, etc.)

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-3	Describe how the Bidder's proposed solution meets the DHHS requirements for unique user ID access. Include: • Specification on configuration of the unique user ID. • How the unique user ID is assigned and managed. • How the unique user ID is used to log system activity. • How the system handles the creation of duplicate user ID accounts.	X			

Response:

- Single Sign On via SAML2 protocol (allows customer to use their own SAML2 compliant identity provider to manage user accounts). This option also supports multi-factor authentication.
- If not using a SAML compliant identity provider for Single Sign On customers can create their own User IDs or they are created by the implementation team. User Ids must be unique.
- User account creation and authentication events are logged.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-4	Describe how the Bidder's proposed solution meets the DHHS standard for administering passwords: • Initial Password assignment. • Strong Password Requirements. • Password reset process. • Password expiration policy. • Password controls for automatic lockout access to any user or user group after an administrator-defined number of unsuccessful log-on attempts.	X			
Response: • Single Sign On via SAML2 protocol allows customers to use their own SAML2 compliant identity provider to manage user accounts and password strength rules. • If not using a SAML compliant identity provider for Single Sign On customers can specify password complexity and account lockout rules.					
SEC-5	Describe how the Bidder's proposed solution supports the use of multi-factor authentication.	X			
Response: • Single Sign On via SAML2 protocol allows customers to use their own SAML2 compliant identity provider to manage multi-factor authentication.					
SEC-6	Describe any security processes for managing security updates, and integrated components subject to vulnerability, including anti-virus.	X			
Response: Centralized OS, anti-virus, and anti-malware update systems are in place and managed by VisualVault team members.					
SEC-7	Describe how the Bidder's proposed solution provides the ability to maintain a directory of all personnel who currently use or access the system.	X			
Response: VisualVault's platform maintains a centralized user directory					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-8	State of Nebraska requires identification and authorization of users through an enterprise directory known as the Nebraska Directory Services (NDS) to access web-based applications. Describe how the Bidder's proposed solution will integrate NDS authentication. Refer to the Nebraska Information Technology Commission Security Architecture – Identification and Authorization – (8-303) for specific requirements: http://nitc.nebraska.gov/standards/8-303.pdf	X			
Response: NDS is based upon Active Directory which is SAML 2 compliant. VisualVault supports Single Sign On (SSO) with Active Directory and other SAML 2 compliant identity providers.					
SEC-9	Describe how the Bidder's proposed solution provides role-based security and allows restricted access to system features, function, screens, fields, database, etc. Role authentication may occur at the directory level, application level, or database level (depending on database platform). Describe the security administration functions integrated into the proposed system that manage role-based access to system functions, features, and data. Include a description of: • How and where the proposed system stores security attributes or roles (e.g., LDAP attributes, database tables, a file). • The interface between the LDAP and the application, if roles are assigned in an LDAP directory. • How roles are created and security is applied to the role based on how and where security attributes are stored (if multiple options describe each). • How groups are defined and how roles and security are applied to each group. • How access limits are applied to screens and data on screens by role or group. • How users are created and assigned to one or more roles or groups. • How role and group creation and assignment activity is logged.	X			
Response: • VisualVault supports role-based security. • Roles may be assigned to groups or users. • Groups and group membership may be maintained within Active Directory (or any SAML2 compliant identity provider) • Group creation and changes are logged • A consistent security assignment process is used throughout the application to assign groups access to features or data					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-10	Describe how the Bidder's proposed solution automatically disconnects based upon inactivity, as required by DHHS Policies and Procedures. Describe how the feature is administered and what effect disconnect has on any activity or transaction in process at the time of disconnection. Refer to DHHS Securing Hardware and Software Standard (DHHS-IT-2018-001A) for specific requirements. http://dhhs.ne.gov/Pages/fin_ist_policies.aspx	X			
Response: Disconnect upon inactivity is a standard product feature. The inactivity timeout period is configurable.					
SEC-11	Describe how the Bidder's proposed solution protects Confidential and Highly Restricted Data from unauthorized access during transmission. Describe transmission safeguards that are integrated into the proposed system to protect data during transmission, including any encryption technology. Refer to DHHS Information Technology (IT) Security Policy (DHHS-IT-2018-001) for specific requirements: http://dhhs.ne.gov/Pages/fin_ist_policies.aspx	X			
Response: Data is encrypted at rest and in transit. For encryption technology detail please see Attachment P - GRM VisualVault Encryption and Key Management.pdf					

SEC-12	The proposed system will process Confidential and Highly restricted Data. Describe the Bidder's auditing functions for all data that is viewed or changed. Describe how the Bidder's proposed solution provides System Auditing functions, including but not limited to: • The user ID of the person who viewed or made the change to the data. • The date and time of the view or change. • The physical, software/hardware and/or network location of the person while viewing or making the change. • The information that was viewed or changed. • The outcome of the event. Refer to DHHS Information Technology (IT) Audit Standard (DHHS-IT-2018-001F) for specific audit requirements: http://dhhs.ne.gov/Pages/fin_ist_policies.aspx	X			
Response: User Id, Date, Time, source IP address, action type (view, edit) are logged each time a user accesses files or forms.					
SEC-13	If the Bidder's proposed solution has the ability to override edits, describe how the solution audits all overridden edits and identifies information including, but not limited to, the login ID, date, and time.	X			
Response: User Id, Date, Time, source IP address, action type (view, edit) are logged each time a user accesses files or forms. This includes override edits.					
SEC-14	Describe how the Bidder's proposed solution produces daily audit trail reports and allows inquiries, showing updates applied to the data.	X			
Response: Object specific audit trails are accessible throughout the system. The integrated report writer can also be used to search, sort, and filter audit trail and event log data.					

SEC-15	Describe how the Bidder's proposed solution provides an auto archive/purge of the log files to prevent uncontrolled growth of the log and historical records storage using administrator-set parameters.	X			
Response: File based logs are imported at 5-minute intervals to a centralized log management system designed for high volumes of data. These log files are then auto purged at configurable intervals.					
SEC-16	Describe how the Bidder's proposed solution supports encryption of data at rest or an equivalent alternative protection mechanism. Describe the proposed encryption of data. If data is not encrypted, describe in detail compensating controls. Refer to DHHS Information Technology (IT) Security Policy (DHHS-IT-2018-001) for specific requirements: http://dhhs.ne.gov/Pages/fin_ist_policies.aspx	X			
Response: Data is encrypted at rest and in transit. For encryption technology detail please see Attachment P - GRM VisualVault Encryption and Key Management.pdf					
SEC-17	Describe how the Bidder's proposed solution adheres to the principle of "Fail Safe" to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks.	X			
Response: User accounts are denied access to resources unless explicitly granted.					

SEC-18	Describe how the Bidder's proposed solution is configurable to prevent corruption or loss of data already entered into the solution in the event of failure.	X			
Response: This is accomplished through automatic revisioning of file and form data. Most changes result in new records vs. an update / overwrite of existing records.					
SEC-19	Describe how the Bidder's proposed solution, prior to access of any Confidential or Highly Restricted Data, displays a configurable warning or login banner. In the event that a solution does not support pre-login capabilities, describe how the solution displays the banner immediately following authorization.	X			
Response: • Application login screen provides configurable message area • For Single Sign On users the customer identity provider (Active Directory,etc.) provides this capability.					
SEC-20	Describe how the Bidder's proposed solution recognizes Confidential and Highly Restricted information in screens, reports and views (i.e. PHI and SSN) by restricting distribution and access based upon system security settings and roles. Describe warning banner on printed and viewed reports.	X			
Response: • Form fields must be designated as confidential which prevent display on screen or when printing.					

SEC-21	Describe how the Bidder's proposed solution alerts staff authorities identified by DHHS of potential violations of security and privacy safeguards and adheres to the DHHS Information Technology (IT) Incident Management Standard (DHHS-IT- 2018-001E) requirements. http://dhhs.ne.gov/Pages/fin_ist_policies.aspx	X			
Response: VisualVault maintains a live system status page available at https://status.visualvault.com where customers may subscribe to downtime, scheduled maintenance, and other system status notification events.					
SEC-22	Describe how the Bidder's proposed solution provides the capability to monitor, identify, and report on events on the information system, detects attacks, and provides identification of unauthorized use and attempts of the system.	X			
Response: VisualVault was originally developed as a compliance application for Medical manufacturers. As such, every action, activity, and attempt to log-in or penetrate the system is automatically recorded and reports can be generated and distributed.					
SEC-23	Describe how the Bidder's proposed solution provides a process for archiving and/or destroying data and sanitizing storage media in conformance with DHHS data governance policies and subject to applicable HIPAA, and federal (e.g., Federal Information Processing Standards (FIPS), National Institutes of Standards and Technology (NIST), and State laws. Refer to DHHS Securing Hardware and Software Standard (DHHS-IT-2018-001A) for specific requirements. http://dhhs.ne.gov/Pages/fin_ist_policies.aspx	X			
Response: The VisualVault platform's core is an Enterprise Content Management (ECM) Suite of services. Records Retention is a core function. The VisualVault repository is a true archive. Once submitted, data and content cannot be changed to assure proper governance. All changes to existing data and content are saved as versions to the original assuring the chain of custody is maintained. Data and content destruction is automated based on retention rules. Lists for DHHS staff are produced showing what is to be destroyed and approval is required prior to destruction being implemented.					

Cloud Data Protection	**Annual SOC2 audit** **HIPAA HITECH (3rd party assessment}** **Vulnerability Assessments by independent 3rd** **party Pen Testing by independent 3rd party** **Routine internal vulnerability scans** **Intrusion Detection Systems**
Data Centers	**SOC2**
Record Centers	**SOC2**
Scanning Centers	**SOC2**
Document Imaging	**SOC2, HIPAA HITECH**
Medical Records	**SOC2, HIPAA HITECH**
Financial Document Management	**SEC 17a-4**
Software Engineering	**ISO 27001 Compliant Processes**
Document Shredding	**SOC2**

Please see:

Attachment A – GRM VisaulVault 2016-Type 2 SOC 2 Report

Attachment B - GRM VisualVualt 2016 HIPAA-HITECH Security Assessment Report

Attachment D - GRM VisualVault Technical Summary

SEC-24	Describe how the Bidder's proposed solution has defined and deployed strong controls (including access and query rights) to prevent any data misuse, such as fraud, marketing or other purposes.				

Response:

Data encryption, audit trails, printing restrictions, export restrictions, multi-factor authentication support, IP address restriction options

SEC-25	Describe how the Bidder's proposed solution supports logging to a common audit engine using the schema and transports specified by DHHS. Describe how the solution exports logs in such a manner as to allow correlation based on time (e.g. Coordinated Universal Time [UTC] synchronization).	X			
Response: Log dates and times are UTC. Log files are written using a common format (Apache log4J/log4Net file format). Additional log listeners can be configured by VisualVault operations staff.					
SEC-26	Describe how the Bidder's proposed solution supports removal of a user's privileges without deleting the user from the solution to ensure a history of user's identity and actions.	X			
Response: The system prevents deletion of user accounts which have history. User accounts may be disabled to prevent access.					

System and User Documentation Requirements

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DOC-1	Describe how the Bidder's proposed solution provides on-line Help for all features, functions, and data element fields, as well as descriptions and resolutions for error messages, using help features including indexing, searching, tool tips, and context-sensitive help topics. Provide a sample copy of five screenshots with on-line help with the bidder's response.	X			
Response: VisualVault has base product platform online help (see attached screenshots). We also build customer and business process specific help manuals for each deployment.					
DOC-2	Describe how the Bidder's proposed solution provides an on-line User Manual with a printable version available. The documentation should include full mock-ups of all screens/windows and provide narratives of the navigation features for each window/screen. Provide a sample copy of five pages of the user manual with the bidder's response.	X			
Response: VisualVault has base product platform online help manual (see attached screenshots). We also build customer and business process specific help manuals for each deployment.					
DOC-3	Describe how the Bidder's proposed solution will have on-line Reporting Manual with a printable version available that includes descriptions, definitions, and layouts for each standard report. Include definitions of all selection criteria parameters and each report item/data element, all field calculations defined in detail, and field and report titles. Provide a sample copy of five pages of the Reporting Manual with the bidder's response.	X			
Response: VisualVault has base product platform online reporting help manual (see attached screenshots). We also build customer and business process specific help manuals for each deployment.					

DOC-4	Describe how the Bidder's proposed solution provides a data dictionary which can be viewed online and kept updated for each modification. Provide a sample copy of five pages of the Data Dictionary with the bidder's response.	X			

Response:

VisualVault has base product platform data dictionary (see attached screenshots). We also build a customer and business process specific data dictionary for each deployment.

Training Requirements

This section presents the overall training requirements that apply to the software. They are not specific to any technology or platform.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TRN-1	Describe the Bidder's proposed solution training plan. Describe how the bidder develops and provides training material to DHHS for initial training and updates to training material for enhancements and changes made to the system. The content of these materials should be consistent with the on-line Help, User Manual, and Reporting Manual.	X			

Response:
VisualVault training will include configuration specifically for Nebraska's SUA Aging Information System Software needs, including Nebraska Aging Management Information System (NAMIS) replacement, case management and services (Mediware@, SAMS), and an information and referral database. client services, care and case management, funding splits, administration requirements, and federal reporting requirements.

Our planning efforts will be guided by a Training Plan which will define required training, define the process for delivering the training, & define the stakeholders who will receive the training. We recommend that Nebraska SUA's Training Plan also incorporate Knowledge Transfer activities–those that define the process for transferring system and technical knowledge/information to the appropriate staff.

The Training Plan will specify tasks, methods, materials, and timelines regarding use of our Solution in the following areas:

- Initial understanding, navigation, and use for all *involved in the defined processes*
- Initial understanding, navigation, for *"train the trainer"* team members
- Initial understanding, navigation of the system for *SUA staff*
- Initial understanding, navigation of the system for e*xternal stakeholder/partner users*
- Initial understanding, navigation of the system for System Administrators (SAs)
- Master VisualVault use for all, including SAs
- Leadership training to familiarize each on navigation, use, with a keen focus on reports and how to use them to improve performance and how to track service improvement
- Use of dashboard and reports to document the expected 15% up to 25% reduction in staff labor hours dedicated to NAMI documentation activities.

The Training Plan will provide the necessary structure and processes for SUA and its stakeholders/partners to develop the knowledge, skills, and abilities necessary to operate our Solution. We recommend submission of a Training Completion and Knowledge Transfer Acknowledgement Report to confirm delivery and completion of transition to SUA operation.

Development

VisualVault's training is designed for the different user groups who have varying education requirements based on system use. We develop our training to maximize the user experience by gaining the knowledge required to transform their workday. We develop training strategies that seek to enhance the student's learning experience by incorporating active learning techniques and leveraging SUA Subject Matter Experts (SMEs). This methodology, which is based on best practices and proven experience, is clear and well-defined to minimize risk and enhance communications of risk items and action plans.

Our training is based on adult learning principles and inclusive of a variety of learning styles. We develop training based on some assumptions about how adults learn (Malcolm S. Knowles):

- Adults want to know why they should learn.
- Adults need to take responsibility.
- Adults bring experience to learning.
- Adults are ready to learn when the need arises.
- Adults are task-oriented.

And adults have different learning styles–visual, auditory, and experiential/kinesthetic. Research confirms that we retain approximately 10% of what we see (visual), 30-40% of what we see and hear (visual and auditory), and 90% of what we see, hear, and do (visual, auditory, and experiential). Our proposed training methods address these issues and include readings, videos/slides, lectures, group discussions, examples, role plays, and practice demonstrations–all three learning styles. Our training types have included on-site classroom curriculum, instructor-led, self-paced and self-study, web-based live and recorded sessions for "external" community users (which we have found to be particularly effective for providers), mobile functionality & use of iForms off-line for field inspectors and investigators, and onsite or remote refresher training. We are accustomed to conducting training on policy and/or business process changes, application builds or releases, special or infrequent procedural updates, gap identification and remediation, and training for leadership on navigation and report use. Materials and manuals (Section 7.4 SOW) to support our training efforts can be customized based on SUA needs and can be provided via web portal, CD, or other appropriate method. Training manuals including an online Quick Reference Guide will be provided documenting the use of the VisualVault solution. This manual will be used in conjunction with the Solutions Training classes listed below. This manual will serve as documentation for how the solution operates at the time it is implemented.

Thus, we use a wide variety of training methods:

- On-site classroom curriculum
- Instructor-led
- Self-Paced and Self-Study
- Web based live and recorded sessions for "external community users such as Providers
- Particularly effective for provider education
- A portion of the training is designed for field inspectors and investigators to use VisualVault mobile functionality and how to use iForms off-line
- Refresher training can be scheduled and performed onsite or remotely
- Policy and/or Business Process changes
- Application Builds or Releases
- Special or Infrequent procedural updates
- Gap identification and remediation.

We customize our training to fit the needs of our customers. Our experience has led us to categorize our training based on the following target audience:

- Mandatory - contractually required for assignment to the project [i.e. HIPAA, Security, Fraud, Waste and Abuse, Rights and Responsibilities, etc.]
- Functional Role/Job Specific - to perform a job or function [i.e. system navigation, processing of various submitted materials, complaint reviews, case tracking, etc.
- Supervisory or Lead - team operations and management
- System Administrative - Learning how to navigate, resolve minor issues, make changes to iForms, workflows, etc.
- Leadership - Educate management on navigation and report use.

Production, Test and Training Requirements

DHHS requires three separate environments (Production, Test, and Training) in order to operate the solution on an ongoing basis:

Test Environment – A test environment is required that mirrors the live production environment, including hardware and software. All data should be de-identified. This test environment will be used to test application changes before they are deployed to production. This step is an important part of quality assurance, where all changes are tested to minimize the risk of adverse reactions in the production environment. While it is necessary to mirror all of the functions of the production environment, it is not necessary to maintain the same load capacity.

Training Environment – A Training environment is also required that allows DHHS to provide hands-on training to users. This environment would allow DHHS to maintain unique de-identified data for use in training and conduct training without interference with the test or production environments. This environment will have occasional use.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PTT-1	Describe how the Bidder's proposed solution supports several environments, include production environment, test environment, and training environment.	X			

Response: VisualVault provides two test environments and one production environment:

- Development
- Sandbox
- Production
- DHHS will have a test environment at https://sandbox.visualvault.com

System testing: System testing, including testing mobile compatibility will be performed using pre-defined test scripts that cover all the functionality of the overall system components being tested. System testing will be accomplished by the VisualVault Team from within the DHHS environment.

- System testing scripts: System test scripts will be created in conjunction with DHHS SME's having expert knowledge of the processes being tested. The system testing scripts will include tests for mobile compatibility. All test scripts will be approved by the state's project team prior to their execution.
- System testing sign-off: System testing evaluation and sign-off is required by the VisualVault Team. Completed system test results shall be presented to DHHS as part of project documentation and prior to commencing any user acceptance testing.

System interface testing: System interface testing will be performed. System interface testing shall be accomplished by the bidder team from within DHHS environment.

- System interface testing scripts: System interface testing will be created in conjunction with DHHS SMEs having expert knowledge of the systems and data being tested. System interface testing will include end-to-end tests verifying the completeness and timeliness of all data exchanged between systems. All test scripts will be approved by the DHHS project team prior to their execution.
- System interface testing sign-off: System interface testing evaluation and sign-off is required by the DHHS team.

Completed test results will be presented to DHHS prior to activation of the interface.

User acceptance testing: User Acceptance testing shall be performed, first, within DHHS' Testing Environment and then, upon approval from DHHS, within DHHS' Production Environment. All User Acceptance testing will be performed by designated DHHS SMEs.

- User acceptance testing scripts: User acceptance testing scripts will be created in conjunction with DHHS SMEs having expert knowledge of the process(s) and data being tested. All test scripts will be approved by the DHHS project team prior to their execution.
- User acceptance testing sign-off: User acceptance testing evaluation and sign-off will be the sole responsibility of DHHS.

PTT-2	Describe how the Bidder's proposed solution supports non-production environments such as testing and training environments containing de-identified data and not include Confidential or Highly Restricted data.	X			

Response: VisualVault provides two test environments and one production environment. VisualVault provides:

- Development
- Sandbox
- Production
- DHHS will have a test environment at https://sandbox.visualvault.com

Once AIS is implemented, the Sandbox environment remains active and available to the community of users to allow each to log in and self-train themselves to continue their education. The Sandbox contains test data to use.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PTT-3	Describe how the Bidder's proposed solution provides the ability to refresh any testing or training environment. Describe whether the refresh process can be completed using DHHS resources or whether the process requires services from the Bidder.	X			

Response:

We maintain a base sandbox (testing/training) and development environment for each customer. At this time refreshing the environment requires DHHS to submit a refresh request via technical support.

Interfaces/Imports/Exports Requirements

The proposed software solution is expected to be able to interface with other computer systems as necessary.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
INT-1	Describe the Bidder's proposed automated approach to managing interfaces. Describe how the proposed solution's interfaces secure and protect the data and the associated infrastructure from a confidentiality, integrity and availability perspective.	X			
Response: VisualVault leverages AWS' cloud that provides industry best practices surrounding data security. Additionally, VisualVault uses a combination of symmetric and asymmetric encryption algorithms called "Envelope Encryption" along with a centralized Key Management Service (KMS) to encrypt data at rest. The algorithm used for symmetric encryption is the Advanced Encryption Standard (AES). The algorithm used for asymmetric encryption is RSA. VisualVault's REST API is protected using industry standard OAUTH2 for authentication and authorization. Additionally, API endpoints can be restricted to specific source IP addresses or network segments. Additional information on data security is included in our Attachment H – GRM VisualVault IT security Standard (STD-001) PDF defines our information security standards.				
INT-2	Describe how the Bidder's proposed solution has the capability to notify System Administrators/system support staff if an interface is not available for any reason.	X			
Response: VisualVault maintains a live system status page available at https://status.visualvault.com where customers may subscribe to downtime, scheduled maintenance, and other system status notification events.					
INT-3	Describe how the Bidder's proposed solution provides necessary Application Programming Interface (API), Web Services, and/or secure file transfers to create interfaces to and from the proposed solution.	X			
Response: VisualVault's REST API provides secure API access to most all system functionality. Example code and developer assistance is available for multiple programming languages including JavaScript, Java, .Net, and Python. We provide code examples and documentation for this at http://developer.visualvault.com/api/v1/SampleCode.					
INT-4	Describe how the Bidder's proposed solution supports data exchanges between components in real-time so that data is always synchronous across the entire solution.	X			
Response: Servers and network equipment synchronized using NTP. We monitor all vital system components using centralized monitoring tools.					

System Performance Requirements

This section describes requirements related to the proposed systems' on-line performance, response times, and sizing from a system architecture standpoint.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PER-1	Describe the Bidder's proposed system performance functionality and monitoring tools.	X			
Response: VisualVault operations uses multiple centralized monitoring tools with KPI's extracted from monitoring data and used to report system performance. Examples of tools used are AWS CloudWatch, ManageEngine, and a data warehouse for log data analysis.					
PER-2	Describe the Bidder's expected minimum response times for the following functions, even at peak load. For example, expected response time will be within two (2) seconds 95% of the time, and under 10 seconds for 100% of the time.	X			
☐ Response: Record Search Time: Expected response within 4 seconds 95% of the time, and under 10 seconds 100% of the time ☐ Record Retrieval Time: Expected response within 4 seconds 95% of the time, and under 10 seconds 100% of the time ☐ Transaction Response Time: (User interface-initiated transactions) Expected response within 4 seconds 95% of the time, and under 10 seconds 100% of the time ☐ Print Initiation Time: Expected response within 4 seconds 95% of the time, and under 10 seconds 100% of the time ☐ Subsequent Page Display Response Time: Expected response within 4 seconds 95% of the time, and under 10 seconds 100% of the time ☐ Document Availability: File download start response within 4 seconds 95% of the time, and under 10 seconds 100% of the time ☐ Report Generation and Ad-hoc Queries: Expected response within 5 seconds 95% of the time, dependent upon data set size.					
PER-3	Describe how the Bidder's proposed solution captures system downtimes, along with the causes of the downtimes where applicable. Describe the Bidder's proposed method and timing of communication to DHHS on downtimes.	X			
Response: VisualVault maintains a live system status page available at https://status.visualvault.com where customers may subscribe to downtime, scheduled maintenance, and other system status notification events.					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PER-4	Describe how the Bidder's proposed solution supports concurrent users with minimal impact to response time, with the ability to increase the demand on the system by 50% without modification to the software or degradation in performance.	X			

Response:

VisualVault load balances application server requests across two AWS availability zones with 100 cross-zone redundancies. Additional capacity may be added by increasing application server node count and/or database server node count.

PER-5	Describe how the Bidder's proposed solution is available online 24 hours a day and 7 days a week, 99.9% of the time each month. Describe any known timeframes where the system will be unavailable for use.	X			

Response:

We schedule maintenance windows with a minimum one-week notice. There is typically no down time for maintenance windows. If downtime is required, the time window is typically 30 minutes or less. Any planned maintenance requiring downtime is announced 2 weeks or more in advance and a notice is placed on the login screens and our system status website. VisualVault schedules maintenance during evening or weekend hours only. If a security event requires system maintenance, advance notification time may be less.

PER-6	Describe how the Bidder's proposed solution provides application performance monitoring and management capabilities, including any key performance indicators (KPI) or other metrics to measure and report system performance for the proposed system.	X			

Response:

VisualVault operations uses multiple centralized monitoring tools with KPI's extracted from monitoring data and used to report system performance. Examples of tools used are AWS CloudWatch, ManageEngine, and a data warehouse for log data analysis.

VisualVault maintains a live system status page available at https://status.visualvault.com where customers may subscribe to downtime, scheduled maintenance, and other system status notification events.

TAB 4

TAB 4

TECHNICAL AND AUDIT DOCUMENTATION

A-LIGN

GRM Information Management Services Inc.
Type 2 SOC 2
2017

GRM

REPORT ON GRM INFORMATION MANAGEMENT SERVICES INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY AND CONFIDENTIALITY

Pursuant to Reporting on Service Organization Controls 2 (SOC 2)
Type 2 examination performed under AT-C 105 and AT-C 205

August 1, 2016 To July 31, 2017

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS AT GRM INFORMATION MANAGEMENT SERVICES INC. RELEVANT TO SECURITY AND CONFIDENTIALITY

To GRM Information Management Services Inc.:

We have examined the attached description titled "Description of GRM Information Management Services Inc.'s Records Management Services System Throughout the Period August 1, 2016 To July 31, 2017" and the suitability of the design and operating effectiveness of controls to meet the criteria for the Security and Confidentiality principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), throughout the period August 1, 2016 to July 31, 2017. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of GRM Information Management Services Inc.'s ('GRM' or 'the Company') controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

GRM has provided the attached assertion titled "Management of GRM Information Management Services Inc.'s Assertion Regarding Its Records Management Services System Throughout the Period August 1, 2016 To July 31, 2017," which is based on the criteria identified in management's assertion. GRM is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in GRM's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period August 1, 2016 to July 31, 2017.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the description criteria identified in GRM's assertion and the applicable trust services criteria

a. the description fairly presents the system that was designed and implemented throughout the period August 1, 2016 to July 31, 2017.
b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period August 1, 2016 to July 31, 2017, and user entities applied the complementary user-entity controls contemplated in the design of GRM's controls throughout the period August 1, 2016 to July 31, 2017.
c. the controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period August 1, 2016 to July 31, 2017.

The specific controls we tested and the nature, timing, and results of our tests are presented in the section of our report titled "Information Provided by the Service Auditor".

This report and the description of tests of controls and results thereof are intended solely for the information and use of GRM; user entities of GRM's Records Management Services System during some or all throughout the period August 1, 2016 to July 31, 2017; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, or other parties.
- Internal control and its limitations.
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

A-LIGN

August 30, 2017
Tampa, Florida

SECTION 2

MANAGEMENT OF GRM INFORMATION MANAGEMENT SERVICES INC.'S ASSERTION REGARDING ITS SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2016 TO JULY 31, 2017

Management of GRM Information Management Services Inc.'s Assertion Regarding Its System Throughout the Period August 1, 2016 to July 31, 2017

August 30, 2017

We have prepared the attached description titled "Description of GRM Information Management Services Inc.'s Records Management Services System Throughout the Period August 1, 2016 To July 31, 2017", based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.34-.35 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the Records Management Services System, particularly system controls intended to meet the criteria for the Security and Confidentiality principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

a. The description fairly presents the Records Management Services System throughout the period August 1, 2016 to July 31, 2017, based on the following description criteria:

   i. The description contains the following information:

      (1) The types of services provided.

      (2) The components of the system used to provide the services, which are the following:

         - *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
         - *Software*. The application programs and IT systems software that supports application programs (operating systems, middleware, and utilities).
         - *People*. The personnel involved in governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
         - *Processes*. The automated and manual procedures.
         - *Data*. Transaction streams, files, databases, tables, and output used or processed by a system.

      (3) The boundaries or aspects of the system covered by the description.

      (4) How the system captures and addresses significant events and conditions.

      (5) The process used to prepare and deliver reports and other information to user entities or other parties.

      (6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization or other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

      (7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system.

      (8) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore.

(9) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(10) Relevant details of changes to the service organization's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in description were suitably designed throughout the specified period to meet the applicable trust services criteria.

c. The controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

Peter Friedman
Director of Safety and Security
GRM Information Management Services Inc.

SECTION 3

DESCRIPTION OF GRM INFORMATION MANAGEMENT SERVICES INC.'S SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2016 TO JULY 31, 2017

OVERVIEW OF OPERATIONS

Company Background

Founded in New York City in 1987, GRM Information Management Services, Inc. (GRM) is currently headquartered in Jersey City, New Jersey. GRM provides records management services to both public and private organizations that require high levels of security and reliability for the physical and digital storage of critical assets.

Description of Services Provided

GRM offerings include records storage, imaging, document shredding, and offsite data storage all within a secure, centralized environment. GRM also provides its clientele the technology of a global enterprise combined with the individual attention of a local operation. GRM offers a complete menu of integrated information management services including Digital Document and Records Management; document imaging/scanning and conversion; outsourced hosting; smart web portals; workflow tracking; image enabling and more.

Medical Records Management

Healthcare and the world of medicine is a practice based on precision, promptness and performance. Taking that cue, GRM has customized a Records and Information Management Solution that incorporates the key factors needed in the medical field while maximizing service offerings. Securely storing medical records, while allowing them to be accurately tracked and available at a moment's notice, is at the core of GRM's Medical Records Management plan.

GRM's Healthcare Information Management Suite seamlessly links every department - Accounting, Billing, Patient Services, Compliance, Medicine, Human Resources, and Information Technology - in order to reduce costs, increase access and improve care. These foundations need to be maintained even as Medical Records Management is migrating to the digital world where Electronic Medical Records (EMR) has become an absolute requirement. The Scan-On-Request service is the optimum method for enhancing any Medical Facility's EMR capabilities. GRM scans and digitally store all records within the eVault system or Online Records Center as well as physically within a Records Center. Documents are available to manage online via eAccess, while still remaining available for physical delivery whenever necessary.

GRM's Medical Records Management System makes it possible for medical or healthcare facilities to:

- Maintain the privacy and security of medical records and patient information
- Government mandates the release of Protected Health Information (PHI)
- Health Insurance Portability and Accountability Act (HIPAA)
- Managing to the complex rules and regulations governing the Release of Information (ROI)
- Ensuring regulatory compliance
- Improving physician productivity by providing better information at the point of care
- Consolidating patient information that is scattered across disparate systems, making it possible to share vital medical, clinical and patient records

Infrastructure

Primary infrastructure used to provide GRM's Records Management Services system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Servers	HP DL380	Host files to support the corporate web application
Firewalls	Cisco ASA 5510	Filter traffic into and out of the private network supporting the corporate services
Switches	HP 2920	Connect devices on the corporate network by sending message to the specific devices that need to receive it
Routers	Cisco 2900 ISR	Connect multiple networks and forward packets within the network or other networks

Software

Primary software used to provide GRM's Records Management Services system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Backup Executive	Windows Server 2012 R2	Performs scheduled backups of client data according to the requirements defined by the customer and provides status alerts to operations personnel
OTRS 3.2	Linux	Provides functionality to document and track issues and requests for the client environment
Nagios	Linux	Monitoring application used to provide monitoring, alert and notification services for the hosted client environments

People

The GRM staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- System administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues
- Security - performs annual risk assessment and provides continuous improvement feedback

Processes

GRM Document Management operates in the Information and Records Management industry. Their end-to-end storage and Information Management Solutions are delivered through their brick-and-mortar facilities using defined processes and procedures.

Secure Records Storage Centers

GRM safely stores and secures sensitive information by maintaining state-of-the-art facilities, employing the latest software and technology. WGRM utilizes over 3 million square feet of storage space spread throughout several Records Management Centers located across the United States - each outfitted to serve as primary business centers capable of accommodating even the most demanding data storage requirements. GRM facilities include the following features:

- 24/7 security, utilizing CCTV and on-premises guards
- Comprehensive fire suppression systems
- Customized shelving to allow for the storage of all size boxes
- Private access rooms for on-site viewing
- Designated staging areas
- Full office amenities
- Document Management Technology

Since GRM's inception, barcode technology has been at the backbone of their information management strategy. Barcoding is the most important step in a record's chain-of-custody. GRM's barcoding ensures that customers have an accurate inventory and that we know the precise location of each and every record. Barcoding also helps ensure complete confidentiality and records compliance.

The process begins by assigning a unique, discrete barcode identification number to each shelf location within the Offsite Data Storage Centers. The same is done for every storage container and, in some cases, even specific documents, assuring 100% accurate tracking, monitoring and delivery. In order to facilitate this process, GRM Records Center personnel and GRM drivers are equipped with laser scanners, as well as portable printers for our drivers, allowing them to print scanner-validated receipts. Trucks are outfitted with wireless radios to maintain contact with GRM's Dispatching Group. All deliveries and pickups are monitored in real time via Digital Dispatch, GRM's proprietary, real-time fleet management and performance software. GRM's full-time, in-house IT Group - including Application Developers, Systems Engineers and Telecommunications Specialists - oversee all of our scanning and Document Management technology.

GRM eAccess, is also offered as the web-based inventory control and order request application, which places complete database capabilities, including online document imaging services and customized activity reports, instantly at clients' fingertips.

Customer Service

In order to meet client needs, live customer assistance with GRM's offsite data protection and Information Management Systems staff is available 24 hours a day - year-round. GRM directs all queries, orders and transactions to clients' local GRM secure offsite Records Management Center. All archiving and retrievals are performed by fully-trained GRM personnel. Drivers adhere to GRM's strict delivery and pick-up procedures and protocols.

GRM offers Next Day and Same Day Delivery services. All deliveries and pickups are scanner-validated for 100% accuracy. And local GRM Account Executive and Client Service Manager are always ready to respond to inquiries.

Cut Costs

Adding to the GRM value equation is the ability to remotely control every aspect of clients' document storage through the eAccess smart web portal. This service, which is FREE to every GRM customer, allows access for managing document inventory conveniently—at any time and from any computer with a web browser. Clients can request pick-ups or deliveries, apply user authorizations, generate reports and much more.

GRM's Scan-On-Request service provides clients with an immediate need for the contents of a stored document. GRM is able to scan documents offsite or onsite, depending on client needs. GRM can also convert a scanned document to virtually any digital format.

For clients that wish to transition much of their information to digital while maintaining some hard copy information, GRM offers the best of both worlds in their Blended Solution. It's an opportunity to consider your entire organization and make recommendations that benefit you across the board, sustaining both paper and digital records as needed. All of these services are delivered in-house.

Improve Productivity

GRM Document Storage organizes and tracks client information, enabling the ability to find what's needed quickly. Productivity is additionally enhanced through the remote inventory control service, eAccess, which is FREE to every GRM customer. eAccess allows clients to manage information any time of day from any location with computer access.

GRM provides an entire range of productivity-enhancing services that save time and effort. Digital Dispatch, allows clients to arrange timely pick-ups and deliveries of documents. The Certified Shredding also helps by eliminating obsolete documents and cost-effectively reducing the quantity of information to manage overall.

GRM can help improve productivity even more by converting hard copies to digital and sending them in a flash electronically. In the digital environment, further workflow efficiency is possible through GRM's single repository web hosting. Here, the GRM Online Record Center secures and stores client information electronically while making it available for a wide range of cost-effective workflow applications.

Reduce Risk

GRM maintains an awareness of existing and new regulatory requirements for information to help meet clients' compliance needs. At GRM, document management expertise extends to a full understanding of compliance issues and relevant compliance legislation that impacts businesses and industries. The PrecisionPLUS barcode tracking lowers risk by ensuring the accuracy and around-the-clock accessibility of documents. By providing a complete, chain-of-custody record, the service ensures that every item is easily, quickly located and that you have a legally defensible response to investigations, audits and lawsuits.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured which is utilized by GRM in delivering its Records Management Services system. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the commercial monitoring applications
- Alert notifications received from automated backup systems
- Incident reports documented via the ticketing systems

Boundaries of the System

The scope of this report includes the Records Management Services system performed in the Chicago, Illinois; Jersey City, New Jersey; Miami, Florida; San Francisco, California; Los Angeles, California; and Philadelphia, Pennsylvania facilities.

Significant Events and Conditions

GRM has implemented automated and manual procedures to capture and address significant event and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the Records Management Services system. Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

Preparation and Delivery of Reports and Data

GRM utilizes the services and procedures described above to capture, prepare, and deliver reports and other information (described in the data section above) to user entities and other parties.

Subservice Organizations

No subservice organizations were included in the scope of this assessment.

Criteria Not Applicable to the System

All Common (Security) and Confidentiality criterion was applicable to the GRM Records Management Services system.

Significant Changes Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization last review.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of GRM's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of GRM's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook
- Background checks are performed for employees as a component of the hiring process

Commitment to Competence

GRM's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge. Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.

Management's Philosophy and Operating Style

GRM's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

GRM's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

GRM's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.

Human Resources Policies and Practices

GRM's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. GRM's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

RISK ASSESSMENT

GRM's risk assessment process identifies and manages risks that could potentially affect GRM's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. GRM identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by GRM, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. GRM attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

TRUST SERVICES PRINCIPLES AND CRITERIA

In-Scope Trust Services Principles

Common Criteria (*to all Security and Confidentiality Principles*)
The security principle refers to the protection of the system resources through logical and physical access control measures in order to enable the entity to meet its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.

Confidentiality
The confidentiality principle addresses the system's ability to protect information designated as confidential, including, its final disposition and removal from the system in accordance with management's commitments and system requirements. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention, and restrict its disclosure to defined parties (including those who may otherwise have authorized access within the boundaries of the system). Such requirements may be contained in laws or regulations, or commitments in user contracts. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that the privacy applies only to personal information, while the confidentiality principle applies to various types of sensitive information. In addition, the privacy principle addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of GRM's Records Management Services system; as well as the nature of the components of the system result in risks that the criteria will not be met. GRM addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, GRM's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Control Activities Specified by the Service Organization

The applicable trust criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of GRM's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

MONITORING

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. GRM's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

GRM's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in GRM's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of GRM's personnel.

Reporting Deficiencies

Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked. Management meetings are held to review reported deficiencies and corrective actions.

INFORMATION AND COMMUNICATION SYSTEMS

Information and communication is an integral component of GRM's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At GRM, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within GRM. Management believes that open communication channels help ensure that exceptions are reported and acted on. Management's communication activities are made electronically, verbally, and through the actions of management.

Specific information systems used to support GRM's Records Management Services system are described in the Description of Services section above.

COMPLEMENTARY USER ENTITY CONTROLS

GRM's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Principles related to GRM's services to be solely achieved by GRM control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of GRM's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Principles described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to GRM.
2. User entities are responsible for notifying GRM of changes made to technical or administrative contact information.
3. User entities are responsible for ensuring the supervision, management and control of the use of GRM services by their personnel.
4. User entities and subservice organizations are responsible for understanding and complying with their contractual obligations to GRM.
5. User entities are responsible for notifying GRM of changes made to technical or administrative contact information.
6. User entities are responsible for maintaining their own system(s) of record.
7. User entities are responsible for ensuring the supervision, management and control of the use of GRM services by their personnel.
8. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize GRM services.
9. User entities are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals.
10. User entities are responsible for ensuring the confidentiality of any user IDs and passwords used to access GRM's systems.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN's examination of the controls of GRM was limited to the Trust Services Principles and related criteria and control activities specified by the management of GRM and did not encompass all aspects of GRM' operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities were performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user entity's transactions;
- Understand the flow of significant transactions through the service organization;
- Determine whether the control objectives are relevant to the user entity's financial statement assertions; and
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user entity's financial statements and determine whether they have been implemented.

Control Activities Specified by the Service Organization

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementetion, operation, maintenance, and monitoring of the system enabling it to meet its commitments and requirements as they relate to security and confidentiality.	A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place to communicate organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Reporting relationships and organizational structures are reviewed periodically by senior management.	Inspected the organizational chart versioning date to determine that reporting relationships and organizational structures were reviewed periodically by senior management.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel.	Inspected a sample of job descriptions to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel.	No exceptions noted.
		Senior management reviews job descriptions on a periodic basis and makes updates, if necessary.	Inspected a sample of job descriptions' revision dates to determine that senior management reviewed job descriptions on a periodic basis and made updates, if necessary.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies, and other system requirements are effectively promulgated and placed in operation.	A documented organizational chart is in place to assign responsibility and delegate lines of authority to personnel.	Inspected the organizational chart to determine that a documented organizational chart was in place to assign responsibility and delegate lines of authority to personnel.	No exceptions noted.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and confidentiality and provides resources necessary for personnel to fulfill their responsibilities.	Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.	Inspected a sample of job descriptions to determine that job requirements were documented in the job descriptions and candidate's abilities to meet the requirements were evaluated as part of the hiring or transfer evaluation process.	No exceptions noted.
		Management documents skills and continued training to establish the organization's commitments and requirements for employees.	Inspected the GRM Information Technology Policy and a sample of training completion certificates to determine that management documented skills and continued training to establish the organization's commitments and requirements for employees.	No exceptions noted.
		Management tracks and monitors compliance with training requirements.	Inspected the GRM training schedule and a sample of training completion certificates to determine that management tracked and monitored compliance with training requirements.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC1.0	**Common Criteria Related to Organization and Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and confidentiality.	Personnel are required to sign and accept the employee handbook acknowledgement and confidentiality agreement upon hire.	Inquired of the director of safety and security regarding employee acknowledgements to determine that personnel were required to sign and accept the employee handbook and confidentiality agreement upon hire.	No exceptions noted.
			Inspected the signed employee handbook acknowledgement forms and confidentiality agreements for a sample of new hires to determine that personnel were required to sign and accept the employee handbook acknowledgement and confidentiality agreement upon hire.	Testing of the control activity disclosed that a confidentiality agreement was not signed within the review period for 1 of the 8 sampled employees.
		Personnel are required to complete a background check provided by a third party vendor upon hire.	Inspected the signed background check authorization forms for a sample of new hires to determine that personnel were required to complete a background check provided by a third party vendor upon hire.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	System descriptions are communicated to authorized external users via service level agreements (SLA) that delineate the boundaries of the system and describe relevant system components.	Inspected sample of client SLAs to determine that system descriptions were communicated to authorized external users via service level agreements that delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		A description of the system delineating its boundaries is posted on the entity's intranet and is available to personnel.	Observed the company intranet to determine that a description of the system delineating its boundaries was posted on the entity's intranet and was available to parsonnel.	No exceptions noted.
		A description of the entity organization structure, system support functions, processes, and organizational roles and responsibilities is posted on the entity's intranet.	Observed the company intranet to determine that a description of the entity organization structure, system support functions, processes, and organizational roles and responsibilities was posted on the entity's intranet.	No exceptions noted.
			Inspected the organizational chart to determine that a description of the entity organization structure, system support functions, processes, and organizational roles and responsibilities was posted on the entity's intranet.	No exceptions noted.
		Customer responsibilities are outlined and communicated through service level agreements.	Inspected a sample of client SLAs to determine that customer responsibilities were outlined and communicated through service level agreements.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.2	The entity's security and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	Security and confidentiality commitments are communicated to external users via defined SLAs.	Inspected a sample of client SLAs to determine that security and confidentiality commitments were communicated to external users via defined SLAs.	No exceptions noted.
		Policy and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the GRM Information Technology Policy to determine that policy and procedures were documented for significant processes and were available on the entity's intranet.	No exceptions noted.
		Management tracks and monitors compliance with training requirements.	Inspected the GRM training schedule and a sample of training completion certificates to determine that management tracked and monitored compliance with training requirements.	No exceptions noted.
		Personnel are required to sign and accept the employee handbook acknowledgement and confidentiality agreement upon hire.	Inspected the signed employee handbook acknowledgement forms and confidentiality agreements for a sample of new hires to determine that personnel were required to sign and accept the employee handbook acknowledgement and confidentiality agreement upon hire.	No exceptions noted.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	Policy and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the GRM Information Technology Policy to determine that policy and procedures were documented for significant processes were available on the entity's intranet.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities are defined in written job descriptions and communicated to personnel.	Inspected a sample of job descriptions to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel.	No exceptions noted.
		Senior management reviews job descriptions on a periodic basis and makes updates, if necessary.	Inspected a sample of job descriptions' revision dates to determine that senior management reviewed job descriptions on a periodic basis and made updates, if necessary.	No exceptions noted.
		Customer responsibilities are outlined and communicated through service level agreements.	Inspected a sample of client SLAs to determine that customer responsibilities were outlined and communicated through service level agreements.	No exceptions noted.
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and confidentiality of the system, is provided to personnel to carry out their responsibilities.	Management documents skills and continued training to establish the organization's commitments and requirements for employees.	Inspected the GRM Information Technology Policy and a sample of training completion certificates to determine that management documented skills and continued training to establish the organization's commitments and requirements for employees.	No exceptions noted.
		Management tracks and monitors compliance with training requirements.	Inspected the GRM training schedule and a sample of training completion certificates to determine that management tracked and monitored compliance with training requirements.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC2.0	**Common Criteria Related to Communications**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.5	Internal and external system users have been provided with information on how to report security and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.	The organization's security policies and code of conduct are communicated to employees in the employee handbook.	Inspected the employee handbook to determine that the organization's security policies and code of conduct were communicated to employees in the employee handbook.	No exceptions noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the GRM Incident Response Policy to determine thet documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		Defined SLAs are in place and communicated to authorized external users regarding procedures for reporting security and confidentiality related failures, incidents, and concerns to personnel.	Inspected a sample of client SLAs to determine that defined SLAs were in place and communicated to authorized external users regarding procedures for reporting security and confidentiality related failures, incidents, and concerns to personnel.	No exceptions noted.
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and confidentiality are communicated to those users in a timely manner.	Security and confidentiality commitments are communicated to external users via defined SLAs.	Inspected a sample of client SLAs to determine that security and confidentiality commitments were communicated to external users via defined SLA.	No exceptions noted.
		Major changes to roles and responsibilities and changes to key personnel are communicated to affected internal users as part of the change management process.	Observed the company intranet to determine that major changes to roles and responsibilities and changes to key personnel were communicated to affected internal users as part of the change management process.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	The entity (1) identifies potential threats that could impair system security and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks.	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.	Inspected the master list of system components to determine that a master list of the entity's system components was maintained, accounting for additions and removals, for management's use.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify threats that could impair system security and confidentielity commitments and requirements.	Inspected the 2017 risk assessment to determine that a formal risk assessment was performed on an annual basis to identify threats that could impair system security and confidentiality commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are reviewed by management.	Inspected the 2017 risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were reviewed by management.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the 2017 risk assessment to determine that management developed risk mitigation strategies to address all risks identified during the risk assessment process.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassasses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the 2017 risk assessment to determine that management had defined a formal risk management process that specified the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		Internal and external vulnerability scans are performed on an annual basis, and remedial actions are taken.	Inspected the vulnerability scan report to determine that internal and external vulnerability scans were performed on an annual basis, and remedial actions were taken.	No exceptions noted.
		Business recovery plans are tested periodically.	Inspected the business continuity program to determine that business recovery plans were tested periodically.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC4.0	**Common Criteria Related to Monitoring of Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and confidentiality and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	Monitoring software is used to identify and evaluate ongoing system performance, securify threats, changing resource utilization needs, and unusual system activity.	Inspected monitoring configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and confidentiality.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the GRM Information Technology Policy to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
		User access to systems is restricted based on role based security defined with an access control system.	Inspected the network user access listing to determine that user access to systems was restricted based on role based security defined with an access control system.	No exceptions noted.
		System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • History (password reuse) • Minimum password age • Password must meet complexity requirements	Inspected the password authentication settings to determine that system users were authenticated via individually-assigned user account and passwords. Production systems were configured to enforce password requirements that included: • Minimum length • History (password reuse) • Minimum password age • Password must meet complexity requirements	No exceptions noted.
		Administrative access is restricted to user accounts accessible by authorized IT personnel.	Inspected the network admin access listing to determine that administrative access was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.	Inspected the master list of system components to determine that a master list of the entity's system components was maintained, accounting for additions and removals, for management's use.	No exceptions noted.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and privacy. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding user access authorization, provisioning, and revocation.	Inspected the GRM Information Technology Policy to determine documented policies and procedures were in place regarding user access authorization, provisioning, and revocation.	No exceptions noted.
		Standardized user access request tickets are utilized to request physical access to the badge access system and logical access to the production systems. Access must be approved by the IT department prior to access being granted.	Inspected the user access request tickets for a sample of new hires to determine that standardized user access request tickets were utilized to request physical access to the badge access system and logical access to the production systems and that access was approved by the IT department prior to access being granted.	No exceptions noted.
		Access to the badge access system (physical access) and production systems (logical access) is revoked as a component of the termination process.	Inspected the user access removal tickets and termination checklists for a sample of terminated employees to determine that access to the badge access system (physical access) and production systems (logical access) was revoked as a component of the termination process.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Account and password sharing is prohibited by company policy.	Inspected the GRM Information Technology Policy to determine that account and password sharing was prohibited by company policy.	No exceptions noted.
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and confidentiality.	User access to systems is restricted based on role based security defined with an access control system.	Inspected the network user access listing to determine that user access to systems was restricted based on role based security defined with an access control system.	No exceptions noted.
		System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • History (password reuse) • Minimum password age • Password must meet complexity requirements	Inspected the password authentication settings to determine that system users were authenticated via individually-assigned user account and passwords. Production systems were configured to enforce password requirements that included: • Minimum length • History (password reuse) • Minimum password age • Password must meet complexity requirements	No exceptions noted.
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and confidentiality.	Documented policies and procedures are in place regarding user access authorization, provisioning, and revocation.	Inspected the GRM Information Technology Policy to determine that to determine that documented policies and procedures were in place regarding user access authorization, provisioning, and revocation.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Standardized user access request tickets are utilized to request physical access to the badge access system and logical access to the production systems. Access must be approved by the IT department prior to access being granted.	Inspected the user access request tickets for a sample of new hires to determine that standardized user access request tickets were utilized to request physical access to the badge access system and logical access to the production systems and that access was approved by the IT department prior to access being granted.	No exceptions noted.
		Access to the badge access system (physical access) and production systems (logical access) is revoked as a component of the termination process.	Inspected the user access removal tickets and termination checklists for a sample of terminated employees to determine that access to the badge access system (physical access) and production systems (logical access) was revoked as a component of the termination process.	No exceptions noted.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and confidentiality.	Documented physical access policies and procedures are in place to guide personnel in physical security practices.	Inspected the GRM facility security procedures to determine that documented physical access policies were in place to guide personnel in physical security practices.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Standardized user access request tickets are utilized to request physical access to the badge access system. Access must be approved by the IT department prior to access being granted.	Inspected the user access request tickets for a sample of new hires to determine that standardized user access request tickets were utilized to request physical access to the badge access system and that access was approved by the IT department prior to access being granted.	No exceptions noted.
		Administrative access within the badge access system is restricted to individually-assigned user accounts accessible by authorized personnel.	Inspected the badge access admin user listing to determine that administrative access within the badge access system was restricted to individually-assigned user accounts accessible by authorized personnel.	No exceptions noted.
		Visitors to the facility are required to be escorted by an authorized employee.	Observed the visitor procedures during walkthrough to determine that visitors to the facility were required to be escorted by an authorized employee.	No exceptions noted.
		Visitors to the facility are required to sign a visitor log upon entering the facility.	Observed the visitor sign in log during facility walkthrough to determine that visitors were required to sign a visitor log upon entering the facility.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Access to the badge access system is revoked as a component of the termination process.	Inspected the user access removal tickets and termination checklists for a sample of terminated employees to determine that access to the badge access system was revoked as a component of the termination process.	No exceptions noted.
		The sharing of access badges is prohibited by company policy.	Inspected the GRM Information Technology Policy to determine that the sharing of access badges was prohibited by company policy.	No exceptions noted.
CC5.6	Logical access security measures have been implemented to protect against security and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	Redundant firewall systems are in place to filter inbound Internet traffic. Traffic not specifically permitted by a firewall rule is denied.	Inspected the network diagram and firewall rulesets to determine that redundant firewall systems were in place to filter inbound traffic and deny any traffic not permitted by the firewall ruleset.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected monitoring configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		Internal and external vulnerability scans are performed on an annual basis, and remedial actions are taken.	Inspected the vulnerability scan report to determine that internal and external vulnerability scans were performed on an annual basis, and remedial actions were taken.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and confidentiality.	SSL encryption technology is used for defined points of connectivity and data transmission.	Inspected the SSL data encryption certificate to determine that SSL encryption technology was used for defined points of connectivity and data transmission.	No exceptions noted.
		Removable media is required to be encrypted by company policy.	Inspected the GRM Information Technology Policy to determine that removable media was required to be encrypted by company policy.	No exceptions noted.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and confidentiality.	Antivirus software is installed on production servers and workstations.	Inspected the antivirus software configurations to determine that antivirus software was installed on production servers and workstations.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC6.0	**Common Criteria Related to System Operations**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.1	Vulnerabilities of system components to security and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and confidentiality.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected monitoring configurations and an example alert notification to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the GRM Incident Response Policy to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		Incremental backups are performed on a daily basis, and full backups are performed on a weekly basis.	Inspected the backup system configurations to determine that incremental backups were performed on a daily basis, and full backups were performed on a weekly basis.	No exceptions noted.
		Antivirus software is installed on production servers and workstations.	Inspected the antivirus software configurations to determine that antivirus software was installed on production servers and workstations.	No exceptions noted.
		Internal and external vulnerability scans are performed on an annual basis, and remedial actions are taken.	Inspected the vulnerability scan report to determine that internal and external vulnerability scans were performed on an annual basis, and remedial actions were taken.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC6.0	**Common Criteria Related to System Operations**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Redundant firewall systems are in place to filter inbound Internet traffic. Traffic not specifically permitted by a firewall rule is denied.	Inspected the network diagram and firewall rulesets to determine that redundant firewall systems were in place to filter inbound traffic and deny any traffic not permitted by the firewall ruleset.	No exceptions noted.
CC6.2	Security, availability, processing integrity, confidentiality and privacy incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the GRM Incident Response Policy to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
		Policies and procedures are in place to address breaches to customer information.	Inspected the customer information breach policy to determine that policies and procedures were in place to address breaches to customer information.	No exceptions noted.
		Entity policies include probation, suspension, and termination as potential sanctions for employee misconduct.	Inspected the GRM Information Technology Policy to determine that entity policies included probation, suspension, and termination as potential sanctions for employee misconduct.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	**Common Criteria Related to Change Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	The entity's commitments and system requirements, as they relate to security and confidentiality are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	A documented SDLC is in place to guide personnel in the handling system changes.	Inspected the GRM Information Technology Policy to determine that a documented SDLC was in place to guide personnel in the handling of system changes.	No exceptions noted.
		System changes are reviewed and approved by management prior to implementation.	Inspected the GRM Information Technology Policy to determine that system changes were reviewed and approved by management prior to implementation.	No exceptions noted.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and confidentiality.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the 2017 risk assessment to determine that management had defined a formal risk management process that specified the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual besis to identify threats that could impair system security and confidentiality commitments and requirements.	Inspected the 2017 risk assessment to determine that a formal risk assessment was performed on an annual basis to identify threats that could impair system security and confidentiality commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are reviewed by management.	Inspected the 2017 risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were reviewed by management.	No exceptions noted.

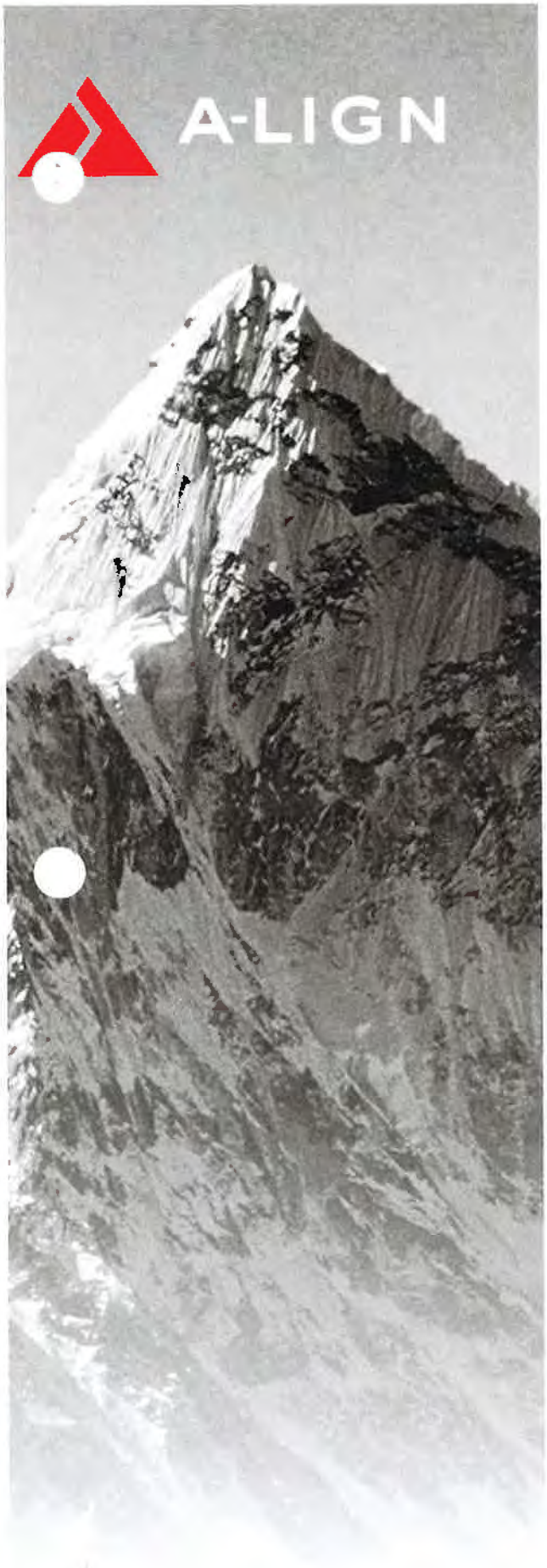
COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	**Common Criteria Related to Change Management**			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the 2017 risk assessment to determine that management developed risk mitigation strategies to address all risks identified during the risk assessment process.	No exceptions noted.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and confidentiality.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident.	Inspected the GRM Incident Response Policy to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.	No exceptions noted.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and confidentiality commitments and system requirements.	A documented SDLC is in place to guide personnel in the handling system changes.	Inspected the GRM Information Technology Policy to determine that a documented SDLC was in place to guide personnel in the handling of system changes.	No exceptions noted.
		System changes and updates are tracked through to successful completion.	Inspected the server update listing to determine that system changes and updates were tracked through to successful completion.	No exceptions noted.
		System changes are reviewed and approved by management prior to implementation.	Inspected the GRM Information Technology Policy to determine that system changes were reviewed and approved by management prior to implementation.	No exceptions noted.

COMMON CRITERIA TO ALL IN SCOPE TRUST SERVICES PRINCIPLES				
CC7.0	Common Criteria Related to Change Management			
Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected monitoring configurations and example alert notification to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.

C1.0	CONFIDENTIALITY CRITERIA			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected monitoring configurations and example alert notification to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		A badge access system is in place to restrict access to highly sensitive areas within the facility, including server rooms and document storage and scanning areas.	Observed the badge access system in place during facilities walkthrough to determine that a badge access system was in place to restrict access to highly sensitive areas within the facility, including server rooms and document storage and scanning areas.	No exceptions noted.
C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.	User access to systems is restricted based on role based security defined with an access control system.	Inspected the network user access listing to determine that user access to systems was restricted based on role based security defined with an access control system.	No exceptions noted.
		Administrative access is restricted to user accounts accessible by authorized IT personnel.	Inspected the network admin access listing to determine that administrative access was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.

C1.0	CONFIDENTIALITY CRITERIA			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A badge access system is in place to restrict access to highly sensitive areas within the facility, including server rooms and document storage and scanning areas.	Observed the badge access system in place during facilities walkthrough to determine that a badge access system was in place to restrict access to highly sensitive areas within the facility, including server rooms and document storage and scanning areas.	No exceptions noted.
C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.	User access to systems is restricted based on role based security defined with an access control system.	Inspected the network user access listing to determine that user access to systems was restricted based on role based security defined with an access control system.	No exceptions noted.
		SSL encryption technology is used for defined points of connectivity and data transmission.	Inspected the SSL data encryption certificate to determine that SSL encryption technologies were used for defined points of connectivity and data transmission.	No exceptions noted.
		Administrative access is restricted to user accounts accessible by authorized IT personnel.	Inspected the network admin access listing to determine that administrative access was restricted to user accounts accessible by authorized IT personnel.	No exceptions noted.
C1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.	Security and confidentiality commitments are communicated to external users via defined SLAs.	Inspected a sample of client SLAs to determine that security and confidentiality commitments were communicated to external users via defined SLAs.	No exceptions noted.

C1.0	CONFIDENTIALITY CRITERIA			
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
C1.5	Compliance with the entity's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.	Document shredding and destruction certificates from third party vendors are obtained and reviewed by management.	Inspected a sample of monthly document shredding and destruction certificates to determine that document shredding and destruction certificates from third party vendors were obtained and reviewed by management.	No exceptions noted.
C1.6	Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.	Security and confidentiality commitments are communicated to external users via defined SLAs.	Inspected a sample of client SLAs to determine that security and confidentiality commitments were communicated to external users via defined SLAs.	No exceptions noted.
C1.7	The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.	The entity establishes written policies related to retention periods for the confidential information it maintains.	Inspected the confidentiality policy to determine that the entity established written policies related to the retention periods for the confidential information it maintained.	No exceptions noted.
C1.8	The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.	The entity: • Disposes of original, archived, backup, and ad hoc or personal copies of records in accordance with its destruction policies • Documents the disposal of confidential information	Inspected the confidentiality policy to determine that the entity: • Disposed of original, archived, backup, and ad hoc or personal copies of records in accordance with its destruction policies • Documented the disposal of confidential information	No exceptions noted.



A-LIGN

GRM Information Management Services, Inc.
Type 1 Attestation (AT-C 105 and AT-C 205)
HIPAA/HITECH
2017

GRM

Table of Contents

SECTION 1

INDEPENDENT PRACTITIONER'S REPORT

INDEPENDENT PRACTITIONER'S REPORT

To GRM Information Management Services, Inc.:

We have examined GRM Information Management Services, Inc.'s ("GRM") assertion that the description of its health information security program for the GRM's Records Management Services System listed in Section 3 (the "description") provided to user entities as of July 31, 2017, is fairly presented and that the health information security program governing the Records Management Services System includes essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009, is presented in accordance with the criteria set forth in GRM's assertion in Section 2. GRM's management is responsible for the assertion. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting the fairness of the presentation of the description and the design of GRM's health information security program for the Records Management Services System and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

A-LIGN did not perform procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon. Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions relevant to meet the applicable HIPAA/HITECH requirements. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable HIPAA/HITECH requirements is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in GRM's assertion in Section 2:

a. The description fairly presents the health information security program for the Records Management Services System that was designed and implemented as of July 31, 2017; and

b. The health information security program governing the Records Management Services System includes essential elements of HIPAA and HITECH

This report and the description of tests of controls and results thereof are intended solely for the information and use of GRM; user entities of GRM's Records Management Services system as of July 31, 2017; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following (which it then bullet points out some items):

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the HIPAA security program
- The HIPAA security program
- The risks that may threaten the achievement of the HIPAA security program and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

A-LIGN

August 30, 2017
Tampa, Florida

SECTION 2

MANAGEMENT'S ASSERTION

GRM

MANAGEMENT'S ASSERTION

August 30, 2017

We have prepared the description of GRM Information Management Services, Inc.' ("GRM") health information security program for the Records Management Services System (the "description") for user entities of the system as of July 31, 2017. We confirm, to the best of our knowledge and belief, that:

a. Management's description fairly presents the health information security program for the Records Management Services System as of July 31, 2017. The criteria we used in making this assertion were that the description:
   i. fairly presents how the health information security program was designed and implemented to govern the security policies and practices supporting the Records Management Services System
   ii. describes the specified controls within the security program designed to achieve the security program's objectives
   iii. does not omit or distort information relevant to the health information security program for the Records Management Services System and may not include every aspect that an individual user entity may consider important in its own particular environment

b. The health information security program governing the Records Management Services System includes essential elements of HIPAA and HITECH. The criteria we used in making this assertion were that:
   i. management determined the applicable controls (the "controls") included in the health information security program
   ii. the controls documented met the standard and implementation guidance for safeguards as defined by the HIPAA Security Rule including the following:
      - Administrative Safeguards;
      - Physical Safeguards;
      - Technical Safeguards;
      - Organizational Requirements; and
      - Breach Notification

Section 3 of this report includes GRM's description of the health information security program for the Records Management Services System that are covered by this assertion.

Peter Friedman
Director of Safety and Security
GRM Information Management Services, Inc.

SECTION 3

DESCRIPTION OF GRM INFORMATION MANAGEMENT SERVICES, INC.'S SYSTEM AS OF JULY 31, 2017

OVERVIEW OF OPERATIONS

Company Background

Founded in New York City in 1987, GRM Information Management Services, Inc. (GRM) is currently headquartered in Jersey City, New Jersey. GRM provides records management services to both public and private organizations that require high levels of security and reliability for the physical and digital storage of critical assets.

Description of Services Provided

GRM offerings include records storage, imaging, document shredding, and offsite data storage all within a secure, centralized environment. GRM also provides its clientele the technology of a global enterprise combined with the individual attention of a local operation. GRM offers a complete menu of integrated information management services including Digital Document and Records Management; document imaging/scanning and conversion; outsourced hosting; smart web portals; workflow tracking; image enabling and more.

Medical Records Management

Healthcare and the world of medicine is a practice based on precision, promptness and performance. Taking that cue, GRM has customized a Records and Information Management Solution that incorporates the key factors needed in the medical field while maximizing service offerings. Securely storing medical records, while allowing them to be accurately tracked and available at a moment's notice, is at the core of GRM's Medical Records Management plan.

GRM's Healthcare Information Management Suite seamlessly links every department - Accounting, Billing, Patient Services, Compliance, Medicine, Human Resources, and Information Technology - in order to reduce costs, increase access and improve care. These foundations need to be maintained even as Medical Records Management is migrating to the digital world where Electronic Medical Records (EMR) has become an absolute requirement. The Scan-On-Request service is the optimum method for enhancing any Medical Facility's EMR capabilities. GRM scans and digitally store all records within the eVault system or Online Records Center as well as physically within a Records Center. Documents are available to manage online via eAccess, while still remaining available for physical delivery whenever necessary.

GRM's Medical Records Management System makes it possible for medical or healthcare facilities to:

- Maintain the privacy and security of medical records and patient information
- Government mandates the release of Protected Health Information (PHI)
- Health Insurance Portability and Accountability Act (HIPAA)
- Managing to the complex rules and regulations governing the Release of Information (ROI)
- Ensuring regulatory compliance
- Improving physician productivity by providing better information at the point of care
- Consolidating patient information that is scattered across disparate systems, making it possible to share vital medical, clinical and patient records

Boundaries of the System

The scope of this report includes the Health Information Security Program for the Records Management Services performed in the Chicago, Illinois; Jersey City, New Jersey; Miami, Florida; San Francisco, California; Los Angeles, California; and Philadelphia, Pennsylvania facilities.

Subservice Organizations

No subservice organizations were included in the scope of this assessment.

HEALTH INFORMATION SECURITY PROGRAM

GRM has developed an information security management program to meet the information security and compliance requirements related to scope of services and its customer base. The program incorporates the elements of the HIPAA and the HITECH. The description below is a summary of safeguards that GRM implemented to adhere to the applicable components of HIPAA Final Security Rule and the breach notification requirements of HITECH.

Administrative Safeguards - policies and procedures designed to show how GRM complies with the act:

- Management has adopted a written set of information security policies and designated the information security officer to be responsible for developing and implementing the required policies and procedures
- Procedures address access authorization, establishment, modification, and termination
- Documented incident response policies for reporting security incidents are in place to guide employees in identifying, reporting, of security incidents
- Business continuity plans are documented to enable continuation of critical business processes in the event of an emergency
- Privileged administrative access to systems is restricted to authorized individuals
- Automated backup systems are in place to perform scheduled replication of production data and systems at pre-defined intervals
- Antivirus software is utilized to detect and eliminate data or files that contain certain virus signatures on certain production servers

Organizational, Policies and Procedures and Documentation - oversight of procedures to protect electronic protected health information according to the act:

- Maintains policies and procedures including, but not limited to, the following
    - Information security policy
    - Asset management
    - Data classification
    - Business continuity
    - Incident management
    - Access control
    - Physical security
- Business associate agreements are documented with third parties and contractors for services that protect the confidentiality, integrity, and availability of the electronic protected health information
- Management ensures policies and procedures regarding the security of electronic private health information are made available to workforce members
- Management documents retention and availability policies to meet minimum requirements
- Management reviews and updates policies and procedures on an annual basis

Physical Safeguards - controlling physical access to protected data:

- Documented physical security policies and procedures are in place to guide personnel in physical security administration
- Physical access procedures are in place restrict access, log visitors, and terminate access to the office facility
- Inventory listings are utilized to track and monitor hardware and removable media
- Data destruction procedures are in place to guide the secure disposal of data and media

Technical Safeguards - controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient:

- Access to in-scope systems are restricted to authorized personnel based on a valid user account and password
- Systems are configured to enforce pre-determined thresholds to lock user sessions due to invalid login attempts
- Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches

Breach Notification - a business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach:

- Documented policies and procedures are in place to guide personnel in notifying the covered entity upon discovery of a breach
- Documented policies and procedures are in place to guide personnel in responding to discovery of a breach
- Documented policies and procedures require disclosure of the unsecured protected health information and include, to the extent possible, the identification of each individual and a description of the event
- Documented policies and procedures are in place to guide personnel in the exception processes of delaying and documenting notifications
- Documented policies and procedures are in place to guide personnel in documentation of administrative requirements for demonstrating that all notifications were made as required

PERIODIC ASSESSMENTS

GRM has a risk assessment process in place to identify and manage the risks that could affect the Company's ability to provide services to its user entities. The risk assessment procedure defines the responsibility, methodologies and processes used by GRM to assess the risks while providing services and develop mitigation strategies to address those risks. This process requires the Company to identify risks based on management's internal knowledge of its operations. The following risk factors are discussed among the executive management at periodic intervals:

- *Risk Assessment*: The risk assessment is performed by the risk management personnel. Risk factors associated with the delivery or implementation of services to customers are evaluated considering process owners, dependencies, timelines and quality
- *Health Information Security Risks*: Health information security risks are assessed by the Director of Safety and Security. Risk factors associated with the organization are evaluated considering compliance obligations, laws and regulations, policies and procedures, contracts and best practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the executive management of the organization

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of GRM's Records Management Services system; as well as the nature of the components of the system result in risks that the requirements will not be met. GRM addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the requirements are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the requirements and the controls necessary to address the risks will be unique. As part of the design and operation of the system, GRM's management identifies the specific risks that the requirements will not be met and the controls necessary to address those risks.

ADMINISTRATIVE SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(1)(i)	**Security management process:** Implement policies and procedures to prevent, detect, contain and correct security violations.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident. Internal and external vulnerability scans are performed on an annual basis, and remedial actions are taken, if necessary.
164.308 (a)(1)(ii) (A)	**Risk analysis:** an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).	A formal risk assessment is performed on an annual basis to identify threats that could impair system security and confidentiality commitments and requirements. Management develops risk mitigation strategies to address risks identified during the risk assessment process.
164.308 (a)(1)(ii) (B)	**Risk management:** Ensures the company implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306. Factors identified in §164.306 include: • The size, complexity, capability of the covered entity • The covered entity's technical infrastructure • The costs of security measures • The probability and criticality of potential risks to ePHI	Identified risks are rated using a risk evaluation process and ratings are reviewed by management. Internal and external vulnerability scans are performed on an annual basis, and remedial actions are taken, if necessary.
164.308 (a)(1)(ii) (C)	**Sanction policy:** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	GRM maintains policy and procedure documents that outline the process of sanctioning personnel who fail to comply with the security policies and procedures.
164.308 (a)(1)(ii) (D)	**Information system activity review:** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.
164.308 (a)(2)	**Assigned security responsibility:** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	A security official is identified as responsible for the development and implementation of the policies and procedures that govern the security of protected ePHI.

ADMINISTRATIVE SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(3)(i)	**Workforce security**: Policies and procedures are implemented to ensure that all members of the workforce have appropriate access to ePHI, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.	User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI. Access to the badge access system (physical access) and production systems (logical access) is revoked as a component of the termination process.
164.308 (a)(3)(ii) (A)	**Authorization and/or supervision**: Ensures the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.	Authorization and/or supervision procedures are in place regarding workforca members who work with ePHI or in locations where it might be accessed. User access to systems is restricted on rola based security defined with an access control system to ensure appropriate access to ePHI.
164.308 (a)(3)(ii) (B)	**Workforce clearance procedure:** Access of a workforce member (employee or computing device) to ePHI is appropriate.	Workforce members have appropriate access to ePHI. User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI.
164.308 (a)(3)(ii) (C)	**Termination procedures:** Ensure that access to ePHI is terminated as soon as possible when a workforce member's employment ends.	Access to the badge access system (physical access) and production systems (logical access) is revoked as a component of the termination process.
164.308 (a)(4)(i)	**Information access management:** Policies and procedures are implemented that ensure authorizing access to ePHI and are consistant with the applicable requirements of the Privacy Rule. Policies and procedures should include: Isolating Health Care Clearinghouse Functions, Access Authorization and Access Establishment and Modification.	User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI.
164.308 (a)(4)(ii) (A)	**Isolating healthcare clearinghouse functions**: If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.	**Not Applicable** - GRM is not a health care clearinghouse.
164.308 (a)(4)(ii) (B)	**Access authorization**: Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI.

ADMINISTRATIVE SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Documented policies and procedures are in place regarding user access authorization, provisioning, and revocation. Standardized user access request tickets are utilized to request physical access to the badge access system and logical access to the production systems. Access must be approved by the IT department prior to access being granted.
164.308 (a)(4)(ii) (C)	**Access establishment and modification:** Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI. Standardized user access request tickets are utilized to request physical access to the badge access system and logical access to the production systems. Access must be approved by the IT department prior to access being granted. Access to the badge access system (physical access) and production systems (logical access) is revoked as a component of the termination process.
164.308 (a)(5)(i)	**Security awareness and training:** Implement a security awareness and training program for all members of the workforce (including management). Component of the Security Awareness and Training program should include Security Reminders, Protection Malicious Software, Log-in Monitoring and Password Management.	Management documents skills and continued training to establish the organization's commitments and requirements for employees.
164.308 (a)(5)(ii) (A)	**Security reminders:** Periodic security updates.	Management tracks and monitors compliance with training requirements.
164.308 (a)(5)(ii) (B)	**Protection from malicious software:** Procedures for guarding against, detecting, and reporting malicious software.	Antivirus software is installed on production servers and workstations. A program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software is in place.
164.308 (a)(5)(ii) (C)	**Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. Documented incident response policies and procedures are in place to guide personnel in the event of an incident.

ADMINISTRATIVE SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(5)(ii) (D)	**Password management**: Procedures for creating, changing, and safeguarding passwords.	Policies are in place to guide personnel in creating, changing, and safeguarding passwords for network devices and servers. System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • Expiration interval • History (password reuse) • Minimum password age • Password must meet complexity requirements
164.308 (a)(6)(i)	**Security incident procedures**: Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident.
164.308 (a)(6)(ii)	**Response and reporting:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
164.308 (a)(7)(i)	**Contingency plan**: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business recovery plans are tested periodically.
164.308 (a)(7)(ii) (A)	**Data backup plan:** Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Documented policy and procedure are in place to guide personnel in performing backups of critical ePHI. Incremental backups are performed on a daily basis, and full backups are performed on a weekly basis.
164.308 (a)(7)(ii) (B)	**Disaster recovery plan**: Establish (and implement as needed) procedures to restore any loss of data.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business recovery plans are tested periodically.
164.308 (a)(7)(ii) (C)	**Emergency Mode Operation Plan:** Establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business recovery plans are tested periodically. Incremental backups are performed on a daily basis, and full backups are performed on a weekly basis.

ADMINISTRATIVE SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(7)(ii) (D)	**Testing and revision procedures**: Implement procedures for periodic testing and revision of contingency plans.	A documented policy on the testing and revision of the business resumption plan and procedure is in place. Business recovery plans are tested periodically.
164.308 (a)(7)(ii) (E)	**Applications and data criticality analysis:** Assess the relative criticality of specific applications and data in support of other contingency plan component.	A formal risk assessment is performed on an annual basis to identify threats that could impair system security and confidentiality commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are reviewed by management.
164.308 (a)(8)	**Evaluation**: Perform a periodic technical and nontechnical evaluation based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of ePHI that establishes the extent to which an entity's security policies and procedures meet the requirement.	A documented policy on the testing and revision of the business resumption plan and procedure is in place. A formal risk assessment is performed on an annual basis to identify threats that could impair system security and confidentiality commitments and requirements. Business recovery plans are tested periodically and updated, if necessary.
164.308 (b)(1)	**Business associate contracts and other arrangements:** A covered entity , in accordance with 164.306 [The Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314 [the Organization Requirements] that the business associate will appropriately safeguard the information.	**Not Applicable** - GRM is not a covered entity.
164.308 (b)(2)	A business associate may permit a business that is a subcontractor to create, receive, maintain, or transmit ePHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	GRM maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.308 (b)(3)	**Written contract or other arrangement:** Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other arrangements with the business associate that meets the applicable requirements of 164.314(a) [the Organizational Requirements].	GRM maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.

ADMINISTRATIVE SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (b)(4)	**Arrangement:** Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other arrangements with the business associate that meets the applicable requirements of 164.314(a).	GRM maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.

PHYSICAL SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.310 (a)(1)	**Facility access controls:** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Documented physical security policies and procedures are in place to guide personnel in physical security practices. A badge access system is in place to restrict access to the facility to authorized personnel. Administrative access within the badge access system is restricted to individually-assigned user accounts accessible by authorized personnel. A video surveillance system is in place with footage retained for at least 90 days. Visitors to the facility are required to sign a visitor log upon entering the facility. Visitors to the facility are required to be escorted by an authorized employee.
164.310 (a)(2)(i)	**Contingency operations:** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business recovery plans are tested periodically.
164.310 (a)(2)(ii)	**Facility security plan:** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Documented physical security policies and procedures are in place to guide personnel in physical security practices.
164.310 (a)(2)(iii)	**Access control and validation procedures:** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	User access to systems is restricted based on role based security defined with an access control system. A badge access system is in place to restrict access to the facility to authorized personnel. Administrative access within the badge access system is restricted to individually-assigned user accounts accessible by authorized personnel. Visitors to the facility are required to be escorted by an authorized employee. Visitors to the facility are required to sign a visitor log upon entering the SOC. A video surveillance system is in place with footage retained for at least 90 days. Access to the badge access system (physical access) and production systems (logical access) is revoked as a component of the termination process.

PHYSICAL SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.310 (a)(2)(iv)	**Maintenance records:** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	Policies and procedures that require the documentation of repairs and modifications to the physical components of a facility are in place.
164.310 (b)	**Workstation use:** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.	Procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI are in place.
164.310 (c)	**Workstation security:** Covered entities should implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.	Procedures are in place to implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.
164.310 (d)(1)	**Device and media control:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	Procedures are in place to ensure that maintenance records of the movements of hardware and electronic media are documented.
164.310 (d)(2)(i)	**Disposal:** Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	Policy and procedure documents that address the final disposition of ePHI require that all ePHI-related media disposal be fully documented.
164.310 (d)(2)(ii)	**Media re-use:** Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. Ensure that ePHI previously stored on electronic media cannot be accessed and reused. Identify removable media and their use. Ensure that ePHI is removed from reusable media before they are used to record new information.	Policy and procedure documents that address the final disposition of ePHI require that all ePHI-related media disposal be fully documented before the media is made available for re-use.
164.310 (d)(2)(iii)	**Accountability:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.
164.310 (d)(2)(iv)	**Data backup and storage:** Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	Incremental backups are performed on a daily basis, and full backups are performed on a weekly basis.

TECHNICAL SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.312 (a)(1)	**Access control:** Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI. Standardized user access request tickets are utilized to request access to the production systems. Access must be approved by the IT department prior to access being granted. System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • Expiration interval • History (password reuse) • Minimum password age • Password must meet complexity requirements Administretive access is restricted to user accounts accessible by authorized IT personnel.
164.312 (a)(2)(i)	**Unique user identification:** Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit end other related business functions.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • Expiration interval • History (password reuse) • Minimum password age • Password must meet complexity requirements
164.312 (a)(2)(ii)	**Emergency access procedure:** Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business recovery plans are tested periodically.
164.312 (a)(2)(iii)	**Automatic logoff:** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Workstations are configured to terminate inactive sessions after a period of inactivity. Users are required to re-validate with a username and password to gain control of the workstation.
164.312 (a)(2)(iv)	**Encryption and decryption:** Implement a mechanism to encrypt and decrypt ePHI.	SSL encryption technology is used for defined points of connectivity and data transmission.
164.312 (b)	**Audit controls**: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.

TECHNICAL SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
164.312 (c)(1)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	Documented shredding and destruction certificates from third party vendors are obtained and reviewed by management. System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • Expiration interval • History (password reuse) • Minimum password age • Password must meet complexity requirements SSL encryption technology is used for defined points of connectivity and data transmission.
164.312 (c)(2)	**Mechanisms to authenticate ePHI:** Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	SSL encryption technology is used for defined points of connectivity and data transmission.
164.312 (d)	**Person or entity authentication**: Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • Expiration interval • History (password reuse) • Minimum password age • Password must meet complexity requirements
164.312 (e)(1)	**Transmission security:** Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	SSL encryption technology is used for defined points of connectivity and data transmission.
164.312 (e)(2)(i)	**Integrity controls:** Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	SSL encryption technology is used for defined points of connectivity and data transmission.
164.312 (e)(2)(ii)	**Encryption:** Implement a mechanism to encrypt ePHI whenever deemed appropriate.	SSL encryption technology is used for defined points of connectivity and data transmission.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.314 (a)(1)	**Business associate contracts or other arrangements:** A covered entity is not in compliance with the standards in § 164.502(e) if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful - (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary."	GRM maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.314 (a)(2)(i)	**Business Associate Contracts:** A business associate contract must provide that the business associate will: "Implement safeguards that protect the confidentiality, integrity, and availability of the electronic protected health...; Report to the covered antity any security incident of which it becomes aware; Authorize termination of the contract, if the covered entity determines that the business associate has violated a material term of the contract."	GRM maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.314 (a)(2)(ii)	**Other Arrangement:** The Other Arrangements implementation specifications provide that when a covered entity and its business associate are both government entities, the covered entity may comply with the standard in either of two alternative ways.	**Not Applicable** - GRM is not a government entity.
164.314 (b)(1)	**Requirements for Group Health Plans:** Except when the only ePHI disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	**Not Applicable** - GRM is not a plan sponsor.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.314 (b)(2)	**Implementation Specifications:** The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to: (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.	**Not Applicable** - GRM is not a plan sponsor.
164.316 (a)	**Policies and Procedures:** Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in 164.306(b)(2)(i), (ii), (iii), and (iv) [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard.	GRM creates and implements appropriate policies and procedures as required by law and as suggested by good business practices and general business ethics. Policies and procedures are reviewed and updated, if necessary; distributed, or otherwise made available to personnel; and are regularly maintained and secured.
164.316 (b)(1)	**Documentation:** Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Documentation is created and maintained in written and electronic form. Actions, activities, or assessments that arise from HIPAA related events are documented in the ticketing system.
164.316 (b)(1)(i)	**Time Limit:** Retain the documentation required by paragraph (b) (1) of this section for 6 years for the date of its creation or the date when it last was in effect, whichever is later.	GRM retains all documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect.
164.316 (b)(1)(ii)	**Availability:** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	HIPAA-related documentation is distributed or made otherwise available to all workforce members.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.316 (b)(1)(iii)	**Updates:** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Documentation is reviewed annually and updated as needed in response to environmental or operation changes affecting the privacy or security of individually identifiable health information.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.402	Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (b)	Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 days after discovery of a breach.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (c)(1)	Elements of the notification required by paragraph (a) of this section shall include to the extent possible: (A)a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) a description of the types of unsecured protected health information that were involved in the breach (Such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (C) any steps the individual should take to protect themselves from potential harm resulting from the breach; (D) a brief description of what the covered entity is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches; and (E) contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an email address, website, or postal address.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.404 (c)(2)	The notification required by paragraph (a) of this section shall be written in plain language.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(1)(i)	The notification required by paragraph (a) shall be provided in the following form: Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(1)(ii)	The notification required by paragraph (a) shall be provided in the following form: If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)	**Substitute notice**. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonable calculated to reach the individual shall be provided. Substitute notice need not be providad in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)(i)	In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)(ii)	In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in tha form of either a conspicuous posting for a period of 90 days on the home page of the web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.404 (d)(3)	In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.406	§164.406(a) For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. (b)Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. (c) The content of the notification required by paragraph (a) shall meet the requirements of §164.404(c).	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (b)	For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, expect as provided in §164.412, provide the notification required by paragraph (a) contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (c)	For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.	**Not Applicable** - GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.410 (a)(1)	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	Breach notification policy and procedures are in place to be used during a breach of ePHI.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.410 (a)(2)	(2) For the purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).	GRM acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.
164.410 (b)	Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.	GRM notifies affected parties of a breach of ePHI no later than sixty (60) calendar days after the discovery of the breach.
164.410 (c)(1)	The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, used or disclosure during the breach.	The identification of each individual whose unsecured ePHI has been accessed during the breach is disclosed during notification procedures.
164.410 (c)(2)	A business associate shall provide the covered entity with any other information that the covered entity is required to include in the notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	Management provides the covered entity with any information that the covered entity is required to include in the notification to the individual at the time of the breach and as soon as it is available.
164.412	If a law enforcement official states to a covered entity or business associate that a notification, notice or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	GRM refrains from, or delays notifying the covered entity, or other required persons following the discovery of a breach of unsecured protected health information when required by law.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.414	**Administrative requirements and burden of proof**: In the event of a use or disclosure in violation of subpart E, the covered entity or business associate; as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402. See §164.530 for definition of breach.	GRM acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.

MONITORING

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. GRM's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

GRM's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in GRM's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of GRM's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

POLICIES AND PROCEDURES

Health information security policies and procedures have been implemented regarding the protection of information assets. The policies and procedures act as a guide for all GRM personnel. These policies and procedures define guidelines for the health information security program related to scope of services, which includes implementing and managing logical access security and controls, including the following:

- Health information security policy
- Asset management
- Data classification
- Business continuity
- Incident management
- Access control
- Physical security

These policies are reviewed and approved by management on at least an annual basis.

Security Awareness Training

GRM employees receive security awareness training for health information security as part of the onboarding process. This training is reinforced by security awareness communications on current issues which are distributed periodically. Additionally, employees are also required to participate in annual security awareness training.

Periodic Testing and Evaluation

GRM completes evaluations throughout each calendar year regarding the effectiveness of the health information security program that include, but are not limited to, the following:

- Internal risk assessments
- Corrective action plans
- Management reviews

Remediation and Continuous Improvement

Areas of non-compliance in GRM's internal control system surface from many sources, including the Company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings, if identified, of internal control non-compliant items should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to areas of non-compliance in internal control procedures and make the decision for addressing any non-compliant items based on whether the incident was isolated or requires a change in the Company's procedures or personnel.

Incident Response

GRM maintains a documented incident response plan including breach notification requirements as mandated by HITECH. The procedures include, but are not limited to, the identification, response, escalation, and remediation of security breaches and other incidents. A formal breach notification process is utilized to document and track resolution of incidents noted. The incident response procedures are tested during the normal course of business and are updated as needed.

COMPLEMENTARY USER ENTITY CONTROLS

GRM Information Management Services, Inc.'s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the HIPAA/HITECH requirements related to GRM Information Management Services, Inc.'s services to be solely achieved by GRM Information Management Services, Inc. control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of GRM Information Management Services, Inc..

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the HIPAA/HITECH requirements described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to GRM.
2. User entities are responsible for notifying GRM of changes made to technical or administrative contact information.
3. User entities are responsible for ensuring the supervision, management and control of the use of GRM services by their personnel.
4. User entities and subservice organizations are responsible for understanding and complying with their contractual obligations to GRM.
5. User entities are responsible for notifying GRM of changes made to technical or administrative contact information.

6. User entities are responsible for maintaining their own system(s) of record.
7. User entities are responsible for ensuring the supervision, management and control of the use of GRM services by their personnel.
8. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize GRM services.
9. User entities are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals.
10. User entities are responsible for ensuring the confidentiality of any user IDs and passwords used to access GRM's systems.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN's examination of the controls of GRM was limited to the HIPAA/HITECH requirements and related control activities specified by the management of GRM and did not encompass all aspects of GRM's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities were performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the HIPAA/HITECH requirements;
- Understand the flow of ePHI through the service organization;
- Determine whether the service organization's controls are suitably designed to meet the health information security program of the user entity's and determine whether they have been implemented.

Voluntary Product Accessibility Template (VPAT)

Date: September 5, 2016
Reviewed: Feb 6, 2017
Name of Product: VisualVault
Product Version: v4.x
Vendor Company Name: GRM Information Management Systems Inc
Vendor Contact Name: Tod Olsen
Vendor Contact Telephone: 480-308-4400

Summary Table

Criteria	Supporting Features	Remarks
Section 1194.21 Software Applications and Operating Systems	**See Section 1194.21 below**	
Section 1194.22 Web-based Internet Information and Applications	**See Section 1194.22 below**	
Section 1194.23 Telecommunications Products	Not Applicable	
Section 1194.24 Video and Multi-media Products	Not Applicable	
Section 1194.25 Self-Contained, Closed Products	Not Applicable	
Section 1194.26 Desktop and Portable Computers	Not Applicable	
Section 1194.31 Functional Performance Criteria	**See Section 1194.31 below**	
Section 1194.41 Information, Documentation and Support	**See Section 1194.41 below**	

Section 1194.21 Software Applications and Operating Systems

Criteria	Supporting Features	Remarks
(a) When software is designed to run on a system that has a keyboard, product functions shall be executable from a keyboard where the function itself or the result of performing a function can be discerned textually.	Supports with Exceptions	Some software functions can only be executed with mouse click or touch screen including the following (not all issues may be listed): • Searching a Document or Form list. Keyboard can be used to perform search but the search input controls do not provide text labels. • Navigating Folder Tree control within the Document Library and File Upload screens can be done using the keyboard but a "hot key" combination is required to select the Folder Tree and begin navigation.
(b) Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer.	Supports	VisualVault does not interfere with or deactivate the accessibility features of the operating system.
(c) A well-defined on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that Assistive Technology can track focus and focus changes.	Supports with Exceptions	Some VisualVault interface elements fail to provide a well-defined on-screen indication of the current focus including the following (not all issues may be listed): • Top level menu items have no clear focus

		with the exception of a drop down menu appearing beneath the top level menu item that is currently in focus.
(d) Sufficient information about a user interface element including the identity, operation and state of the element shall be available to Assistive Technology. When an image represents a program element, the information conveyed by the image must also be available in text.	Supports with Exceptions	Most VisualVault screens expose the necessary information to assistive technologies, with some exceptions including the following (not all issues may be listed): • Form design screen (required only by limited number of admin users). • Additions and removals from lists. • The presence of the context menu is not announced to assistive technology.
(e) When bitmap images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance.	Supports with Exceptions	Bitmap images are used consistently across the VisualVault application with some exceptions (all issues may not be listed): • The iForm electronic signature feature, the image used to initiate the e-sign process does not currently have visible text when in high contrast mode.
(f) Textual information shall be provided through operating system functions for displaying text. The minimum information that shall be made available is text content, text input caret location, and text attributes.	Supports	Text information is correctly exposed in VisualVault.
(g) Applications shall not override user selected contrast and color selections and other individual display attributes.	Supports with Exceptions	VisualVault does not override high contrast mode. Compatibility with high-contrast mode is supported with the following exceptions (all issues may not be listed): • Not all icon images are visible in high-contrast mode but there is associated text which is visible.

(h) When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user.	Not Applicable	
(i) Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	Supports	VisualVault does not rely on color coding as the only means of conveying information.
(j) When a product permits a user to adjust color and contrast settings, a variety of color selections capable of producing a range of contrast levels shall be provided.	Not applicable	
(k) Software shall not use flashing or blinking text, objects, or other elements having a flash or blink frequency greater than 2 Hz and lower than 55 Hz.	Not applicable	
(l) When electronic forms are used, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	Supports with exceptions	Most VisualVault electronic form functionality is accessible to assistive technologies, with some exceptions including the following (all issues may not be listed): • The presence of the context menu is not announced to assistive technology. The context menu is not required to use application features but acts as an alternative method of initiating actions.

Section 1194.22 Web-based Internet Information and Applications

Criteria	Supporting Features	Remarks
(a) A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).	Supports with exceptions	A text equivalent is present for most non-text elements. Exceptions include the following (not all issues may be listed): • Searching a Document or Form list. Keyboard can be used to perform search but the search input controls do not provide text labels. • The iForm electronic signature feature, the image used to initiate the e-sign process does not currently have visible text when in high contrast mode.
(b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.	Not applicable	VisualVault does not use multimedia for presentation.
(c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.	Supports	VisualVault does not rely on color as the only method for conveying information. It is possible for an iForm to be designed so that color is the only indication of state; this is entirely up to the person designing the form.
(d) Documents shall be organized so they are readable without requiring an associated style sheet.	Not applicable	VisualVault does not require a style sheet for reading documents.

(e) Redundant text links shall be provided for each active region of a server-side image map.	Supports	VisualVault does not use image maps.
(f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.	Supports	VisualVault does not use image maps.
(g) Row and column headers shall be identified for data tables.	Supports	VisualVault identifies headers for data tables.
(h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.	Supports with exceptions	VisualVault does not use complex data tables with the following exceptions (not all issues may be listed): • Training Log • iForm Change Log • Workflow Design screen
(i) Frames shall be titled with text that facilitates frame identification and navigation.	Supports	System generated frames are correctly titled. It is possible for an end user to create frames using the iForms designer or the Portal admin screen which are not properly labeled; this is entirely up to the end-user or person designing the iForm or Portal screen.

(j) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	Supports	
(k) A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.	Not applicable	
(l) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by assistive technology.	Supports	All core functionality of VisualVault that relies on scripting is accessible. It is possible for an end user to create Script in the iForms designer which does not create functional text when creating user interface elements; this is entirely up to the end-user or person designing the iForm scripts.
(m) When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with §1194.21(a) through (l).	Not applicable	The VisualVault web application does not require a plug-in for core functionality.
(n) When electronic forms are designed to be completed online, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	Supports with exceptions	Most VisualVault electronic form functionality is accessible to assistive technologies, with some exceptions including the following (all issues may not be listed): • The presence of the context menu is not announced to assistive technology.
(o) A method shall be provided that permits users to skip repetitive navigation links.	Supports	VisualVault provides 'First Page' and 'Last Page' navigation links for list with repetitive navigation links.

(p) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.	Supports	VisualVault has only one timed response feature which is the session end timer. The session end timer provides a textual alert and provides 30 seconds to select the OK button to continue the current session.

Section 1194.31 Functional Performance Criteria

Criteria	Supporting Features	Remarks
(a) At least one mode of operation and information retrieval that does not require user vision shall be provided, or support for Assistive Technology used by people who are blind or visually impaired shall be provided.	Supports	The core functionality of the VisualVault web application is accessible to assistive technology.
(b) At least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 shall be provided in audio and enlarged print output working together or independently, or support for Assistive Technology used by people who are visually impaired shall be provided.	Supports	The core functionality of Google Docs supports the use of screen magnifiers.
(c) At least one mode of operation and information retrieval that does not require user hearing shall be provided, or support for Assistive Technology used by people who are deaf or hard of hearing shall be provided	Not Applicable	No hearing requirements in application.
(d) Where audio information is important for the use of a product, at least one mode of operation and information retrieval shall be provided in an enhanced auditory fashion, or support for assistive hearing devices shall be provided.	Not Applicable	No audio functionality in application.
(e) At least one mode of operation and information retrieval that does not require user speech shall be provided, or support for Assistive Technology used by people with disabilities shall be provided.	Not Applicable.	No speech requirements in application.

(f) At least one mode of operation and information retrieval that does not require fine motor control or simultaneous actions and that is operable with limited reach and strength shall be provided.	Supports with exceptions	Some application functions can only be executed with mouse click or touch screen including the following (not all issues may be listed): • Searching a Document or Form list. Keyboard can be used to perform search but the search input controls do not provide text labels. • Navigating Folder Tree control within the Document Library and File Upload screens can be done using the keyboard but a "hot key" combination is required to select the Folder Tree and begin navigation.

Section 1194.41 Information, Documentation and Support

Criteria	Supporting Features	Remarks
(a) Product support documentation provided to end-users shall be made available in alternate formats upon request, at no additional charge	Supports	
(b) End-users shall have access to a description of the accessibility and compatibility features of products in alternate formats or alternate methods upon request, at no additional charge.	Supports	A copy of this document is available on request at no additional charge
(c) Support services for products shall accommodate the communication needs of end-users with disabilities.	Supported with exceptions	Support is available by email and phone

A-LIGN

GRM INFORMATION MANAGEMENT SERVICES, INC.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) AND THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (HITECH) ASSESSMENT

2016

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports ®

GRM

TABLE OF CONTENTS

SECTION 1

INDEPENDENT PRACTITIONER'S REPORT

A-LIGN

INDEPENDENT PRACTITIONER'S REPORT

To GRM Information Management Services, Inc.:

We have examined GRM Information Management Services, Inc.'s ("GRM") assertion that the description of its health information security program for the GRM Information Management Services, Inc. Records Management Services listed in Section 3 (the "description") provided to user entities as of July 31, 2016, is fairly presented and that the health information security program governing the Records Management Services includes essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009, is presented in accordance with the criteria set forth in GRM Information Management Services, Inc. assertion in Section 2. GRM Information Management Services, Inc. management is responsible for the assertion. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting the fairness of the presentation of the description and the design of GRM Information Management Services, Inc. health information security program for the Records Management Services and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of their nature, GRM Information Management Services, Inc. health information security program may not prevent, or detect and correct, all errors or omissions relevant to the health information security program for the Records Management Services. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design of the health information security program is subject to the risk that controls at GRM may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in GRM Information Management Services, Inc. assertion in Section 2:

a. The description fairly presents the health information security program for the Records Management Services that was designed and implemented as of July 31, 2016; and
b. The health information security program governing the Records Management Services includes essential elements of HIPAA and HITECH

This report, including the description of controls in Section 4, is intended solely for the information and use of GRM and user entities of GRM Information Management Services, Inc. Records Management Services as of July 31, 2016. This report is not intended to be and should not be used by anyone other than these specified parties.

A-LIGN

August 15, 2016
Tampa, Florida

SECTION 2

MANAGEMENT'S ASSERTION

GRM

MANAGEMENT'S ASSERTION

We have prepared the description of GRM Information Management Services, Inc.' ("GRM") health information security program for the Records Management Services (the "description") for user entities of the system as of July 31, 2016. We confirm, to the best of our knowledge and belief, that:

a. Management's description fairly presents the health information security program for the Records Management Services as of August 15, 2016. The criteria we used in making this assertion were that the description:
   i. fairly presents how the health information security program was designed and implemented to govern the security policies and practices supporting the Records Management Services
   ii. describes the specified controls within the security program designed to achieve the security program's objectives
   iii. does not omit or distort information relevant to the health information security program for the Records Management Services and may not include every aspect that an individual user entity may consider important in its own particular environment

b. The health information security program governing the Records Management Services includes essential elements of HIPAA and HITECH. The criteria we used in making this assertion were that:
   i. management determined the applicable controls (the "controls") included in the health information security program
   ii. the controls documented met the standard and implementation guidance for safeguards as defined by the HIPAA Security Rule including the following:
      - Administrative Safeguards;
      - Physical Safeguards;
      - Organizational Requirements
      - Breach Notification

Section 3 of this report includes GRM Information Management Services, Inc. description of the health information security program for the Records Management Services that are covered by this assertion.

Peter Friedman
Director of Safety and Security
GRM Information Management Services, Inc.

SECTION 3

DESCRIPTION OF GRM'S SYSTEM AS OF JULY 31, 2016

OVERVIEW OF OPERATIONS

Company Background

Founded in New York City in 1987, GRM Information Management Services, Inc. (GRM) is currently headquartered in Jersey City, New Jersey. GRM provides records management services to both public and private organizations that require high levels of security and reliability for the physical and digital storage of critical assets.

Description of Services Provided

GRM offerings include records storage, imaging, document shredding, and offsite data storage all within a secure, centralized environment. GRM also provides its clientele the technology of a global enterprise combined with the individual attention of a local operation. GRM offers a complete menu of integrated information management services including Digital Document and Records Management; document imaging/scanning and conversion; outsourced hosting; smart web portals; workflow tracking; image enabling and more.

Medical Records Management

Healthcare and the world of medicine is a practice based on precision, promptness and performance. Taking that cue, GRM has customized a Records and Information Management Solution that incorporates the key factors needed in the medical field while maximizing service offerings. Securely storing medical records, while allowing them to be accurately tracked and available at a moment's notice, is at the core of GRM's Medical Records Management plan.

GRM's Healthcare Information Management Suite seamlessly links every department - Accounting, Billing, Patient Services, Compliance, Medicine, Human Resources, and Information Technology - in order to reduce costs, increase access and improve care. These foundations need to be maintained even as Medical Records Management is migrating to the digital world where Electronic Medical Records (EMR) has become an absolute requirement. The Scan-On-Request service is the optimum method for enhancing any Medical Facility's EMR capabilities. GRM scans and digitally store all records within the eVault system or Online Records Center as well as physically within a Records Center. Documents are available to manage online via eAccess, while still remaining available for physical delivery whenever necessary.

GRM's Medical Records Management System makes it possible for medical or healthcare facilities to:

- Maintain the privacy and security of medical records and patient information
- Government mandates the release of Protected Health Information (PHI)
- Health Insurance Portability and Accountability Act (HIPAA)
- Managing to the complex rules and regulations governing the Release of Information (ROI)
- Ensuring regulatory compliance
- Improving physician productivity by providing better information at the point of care
- Consolidating patient information that is scattered across disparate systems, making it possible to share vital medical, clinical and patient records

HEALTH INFORMATION SECURITY PROGRAM

GRM has developed an information security management program to meet the information security and compliance requirements related to scope of services and its customer base. The program incorporates the elements of the HIPAA and the HITECH. The description below is a summary of safeguards that GRM implemented to adhere to the applicable components of HIPAA Final Security Rule and the breach notification requirements of HITECH.

Administrative Safeguards - policies and procedures designed to show how GRM complies with the act:

- Management has adopted a written set of information security policies and designated the information security officer to be responsible for developing and implementing the required policies and procedures
- Procedures address access authorization, establishment, modification, and termination
- Documented incident response policies for reporting security incidents are in place to guide employees in identitying, reporting, of security incidents
- Business continuity plans are documented to enable continuation of critical business processes in the event of an emergency
- Privileged administrative access to systems is restricted to authorized individuals
- Automated backup systems are in place to perform scheduled replication of production data and systems at pre-defined intervals
- Antivirus software is utilized to detect and eliminate data or files that contain certain virus signatures on certain production servers

Physical Safeguards - controlling physical access to protected data:

- Documented physical security policies and procedures are in place to guide personnel in physical security administration
- Physical access procedures are in place restrict access, log visitors, and terminate access to the office facility
- Inventory listings are utilized to track and monitor hardware and removable media
- Data destruction procedures are in place to guide the secure disposal of data and media

Technical Safeguards - controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient:

- Access to in-scope systems are restricted to authorized personnel based on a valid user account and password
- Systems are configured to enforce pre-determined thresholds to lock user sessions due to invalid login attempts
- Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches

Breach Notification - a business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach:

- Documented policies and procedures are in place to guide personnel in notifying the covered entity upon discovery of a breach
- Documented policies and procedures are in place to guide personnel in responding to discovery of a breach
- Documented policies and procedures require disclosure of the unsecured protected health information and include, to the extent possible, the identification of each individual and a description of the event
- Documented policies and procedures are in place to guide personnel in the exception processes of delaying and documenting notifications
- Documented policies and procedures are in place to guide personnel in documentation of administrative requirements for demonstrating that all notifications were made as required

Periodic Assessments

GRM has a risk assessment process in place to identify and manage the risks that could affect the Company's ability to provide services to its user entities. The risk assessment procedure defines the responsibility, methodologies and processes used by GRM to assess the risks while providing services and develop mitigation strategies to address those risks. This process requires the Company to identify risks based on management's internal knowledge of its operations. The following risk factors are discussed among the executive management at periodic intervals:

- *Risk Assessment*: The risk assessment is performed by the risk management personnel. Risk factors associated with the delivery or implementation of services to customers are evaluated considering process owners, dependencies, timelines and quality
- *Health Information Security Risks*: Health information security risks are assessed by the Director of Safety and Security. Risk factors associated with the organization are evaluated considering compliance obligations, laws and regulations, policies and procedures, contracts and best practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the executive management of the organization

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of GRM's Records Management Services system; as well as the nature of the components of the system result in risks that the requirements will not be met. GRM addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the requirements are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the requirements and the controls necessary to address the risks will be unique. As part of the design and operation of the system, GRM's management identifies the specific risks that the requirements will not be met and the controls necessary to address those risks.

Control Activities Specified by the Service Organization

The applicable requirements, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable requirements and related control activities are included in Section 4, they are, nevertheless, an integral part of GRM's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

ADMINISTRATIVE SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.308 (a)(1)(i)	**Security management process:** Implement policies and procedures to prevent, detect, contain and correct security violations.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident. Internal and external vulnerability scans are performed on an annual basis, and remedial actions are taken, if necessary.
164.308 (a)(1)(ii)(A)	**Risk analysis:** an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).	A formal risk assessment is performed on an annual basis to identify threats that could impair system security and confidentiality commitments and requirements. Manegement develops risk mitigation strategies to address risks identified during the risk assessment process.
164.308 (a)(1)(ii)(B)	**Risk management:** Ensures the company implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306. Factors identified in §164.306 include: • The size, complexity, capability of the covered entity • The covered entity's technical infrastructure • The costs of security measures • The probability and criticality of potential risks to ePHI	Identified risks are rated using a risk evaluation process end ratings are reviewed by management. Internal and external vulnerability scans are performed on an annual basis, and remedial actions are taken, if necessary.
164.308 (a)(1)(ii)(C)	**Sanction policy:** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	GRM maintains policy and procedure documents that outline the process of sanctioning personnel who fail to comply with the security policies and procedures.
164.308 (a)(1)(ii)(D)	**Information system activity review:** Implement procedures to regularly review records of informetion system activity, such as audit logs, access reports, and security incident tracking reports.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.
164.308 (a)(2)	**Assigned security responsibility:** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	The Director of Safety and Security is responsible for the development and implementation of the policies and procedures that govern the security of protected ePHI.
164.308 (a)(3)(i)	**Workforce security:** Policies and procedures are implemented to ensure that all members of the workforce have appropriate access to ePHI, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.	User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI. Access to the badge access system (physical access) and production systems (logical access) is revoked as a component of the termination process.

ADMINISTRATIVE SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.308 (a)(3)(ii)(A)	**Authorization and/or supervision:** Ensures the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.	Authorization and/or supervision procedures are in place regarding workforce members who work with ePHI or in locations where it might be accessed. User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI.
164.308 (a)(3)(ii)(B)	**Workforce clearance procedure:** Access of a workforce member (employee or computing device) to ePHI is appropriate.	Workforce members have appropriate access to ePHI. User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI.
164.308 (a)(3)(ii)(C)	**Termination procedures:** Ensure that access to ePHI is terminated as soon as possible when a workforce member's employment ends.	Access to the badge access system (physical access) and production systems (logical access) is revoked as a component of the termination process.
164.308 (a)(4)(i)	**Information access management:** Policies and procedures are implemented that ensure authorizing access to ePHI and are consistent with the applicable requirements of the Privacy Rule. Policies and procedures should include: Isolating Health Care Clearinghousa Functions, Access Authorization and Access Establishment and Modification.	User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI.
164.308 (a)(4)(ii)(A)	**Isolating healthcare clearinghouse functions:** If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.	**Not Applicable** - GRM is not a health care clearinghouse.
164.308 (a)(4)(ii)(B)	**Access authorization:** Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI. Documented policies and procedures are in place regarding user access authorization, provisioning, and revocation. Standardized user access request tickets are utilized to request physical access to the badge access system and logical access to the production systems. Access must be approved by the IT department prior to access being granted.

ADMINISTRATIVE SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.308 (a)(4)(ii)(C)	**Access establishment and modification:** Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to e workstation, transaction, program, or process.	User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI. Standardized user access request tickets are utilized to request physical access to the badge access system and logical access to the production systems. Access must be approved by the IT department prior to access being granted. Access to the badge access system (physical access) and production systems (logical access) is revoked as a component of the termination process.
164.308 (a)(5)(i)	**Security awareness and training**: Implement a security awareness and training program for all members of the workforce (including management). Component of the Security Awareness and Training program should include Security Reminders, Protection Malicious Software, Log-in Monitoring and Password Management.	Management documents skills and continued training to establish the organization's commitments and requirements for employees.
164.308 (a)(5)(ii)(A)	**Security reminders**: Periodic security updates.	Management tracks and monitors compliance with training requirements.
164.308 (a)(5)(ii)(B)	**Protection from malicious software:** Procedures for guarding against, detecting, and reporting malicious software.	Antivirus software is installed on production servers and workstations. A program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software is in place.
164.308 (a)(5)(ii)(C)	**Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. Documented incident response policies and procedures are in place to guide personnel in the event of an incident.
164.308 (a)(5)(ii)(D)	**Password management:** Procedures for creating, changing, and safeguarding passwords.	Policies are in place to guide personnel in creating, changing, and safeguarding passwords for network devices and servers. System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • Expiration interval • History (password reuse) • Minimum password age • Password must meet complexity requirements

ADMINISTRATIVE SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.308 (a)(6)(i)	**Security incident procedures:** Implement policies end procedures to address security incidents. Policies and procedures should include response reporting.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident.
164.308 (a)(6)(ii)	**Response and reporting:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
164.308 (a)(7)(i)	**Contingency plan:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business recovery plans are tested periodically.
164.308 (a)(7)(ii)(A)	**Data backup plan:** Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Documented policy and procedure are in place to guide personnel in performing backups of critical ePHI. Incremental backups are performed on a daily basis, and full backups are performed on a weekly basis.
164.308 (a)(7)(ii)(B)	**Disaster recovery plan:** Establish (and implement as needed) procedures to restore any loss of data.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business recovery plans are tested periodically.
164.308 (a)(7)(ii)(C)	**Emergency Mode Operation Plan:** Establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business recovery plans are tested periodically. Incremental backups are performed on a daily basis, and full backups are performed on a weekly basis.
164.308 (a)(7)(ii)(D)	**Testing and revision procedures:** Implement procedures for periodic testing and revision of contingency plans.	A documented policy on the testing and revision of the business resumption plan and procedure is in place. Business recovery plans are tested periodically.
164.308 (a)(7)(ii)(E)	**Applications and data criticality analysis:** Assess the relative criticality of specific applications and data in support of other contingency plan component.	A formal risk assessment is performed on an annual basis to identify threats that could impair system security and confidentiality commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are reviewed by management.

ADMINISTRATIVE SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.308 (a)(8)	**Evaluation:** Perform a periodic technical and nontechnical evaluation based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of ePHI that establishes the extent to which an entity's security policies and procedures meet the requirement.	A documented policy on the testing and revision of the business resumption plan and procedure is in place. A formal risk assessment is performed on an annual basis to identify threats that could impair system security and confidentiality commitments and requirements. Business recovery plans are tested periodically and updated, if necessary.
164.308 (b)(1)	**Business associate contracts and other arrangements:** A covered entity, in accordance with 164.306 [The Security Standards: General Rules], may permit a business associate to craate, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314 [the Organization Requirements] that the business associate will appropriately safeguard the information.	**Not Applicable** - GRM is not a covered entity.
164.308 (b)(2)	A business associate may permit a business that is a subcontractor to create, receive, maintain, or transmit ePHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	GRM maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.308 (b)(3)	**Written contract or other arrangement:** Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other arrangements with the business associate that meets the applicable requirements of 164.314(a) [the Organizational Requirements].	GRM maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.308 (b)(4)	**Arrangement:** Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other arrangements with the business associate that meets the applicable requirements of 164.314(a).	GRM maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.

PHYSICAL SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.310 (a)(1)	**Facility access controls:** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Documented physical security policies and procedures are in place to guide personnel in physical security practices. A badge access system is in place to restrict access to the facility to authorized personnel. Administrative access within the badge access system is restricted to individually-assigned user accounts accessible by authorized parsonnel. A video surveillance system is in place with footage retained for at least 90 days. Visitors to the facility are required to sign a visitor log upon entering the facility. Visitors to the facility are required to be escorted by an authorized employee.
164.310 (a)(2)(i)	**Contingency operations:** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode oparations plan in the event of an emergency.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business recovary plans are tested periodically.
164.310 (a)(2)(ii)	**Facility security plan:** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Documented physical security policies and procedures are in place to guide personnel in physical security practices.
164.310 (a)(2)(iii)	**Access control and validation procedures:** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	User access to systems is restricted based on role based security defined with an access control system. A badge access system is in place to restrict access to the facility to authorized personnel. Administrative access within the badge access system is restricted to individually-assigned user accounts accessible by authorized personnel. Visitors to the facility are required to be escorted by an authorized employee. Visitors to the facility are required to sign a visitor log upon entering the SOC. A video surveillance system is in place with footage retained for at least 90 days. Access to the badge access system (physical access) and production systems (logical access) is revoked as a component of the termination process.

PHYSICAL SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.310 (a)(2)(iv)	**Maintenance records:** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	Policies and procedures that require the documentation of repairs and modifications to the physical components of a facility are in place.
164.310 (b)	**Workstation use:** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.	Procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI are in place.
164.310 (c)	**Workstation security:** Covered entities should implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.	Procedures are in place to implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.
164.310 (d)(1)	**Device and media control:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	Procedures are in place to ensure that maintenance records of the movements of hardware and electronic media are documented.
164.310 (d)(2)(i)	**Disposal:** Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	Policy and procedure documents that address the final disposition of ePHI require that all ePHI-related media disposal be fully documented.
164.310 (d)(2)(ii)	**Media re-use:** Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. Ensure that ePHI previously stored on electronic media cannot be accessed and reused. Identify removable media and their use. Ensure that ePHI is removed from reusable media before they are used to record new information.	Policy and procedure documents that address the final disposition of ePHI require that all ePHI-related media disposal be fully documented before the media is made available for re-use.
164.310 (d)(2)(iii)	**Accountability:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.
164.310 (d)(2)(iv)	**Data backup and storage:** Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	Incremental backups are performed on a daily basis, and full backups are performed on a weekly basis.

TECHNICAL SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.312 (a)(1)	**Access control:** Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	User access to systems is restricted on role based security defined with an access control system to ensure appropriate access to ePHI. Standardized user access request tickets are utilized to request access to the production systems. Access must be approved by the IT department prior to access being granted. System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • Expiration interval • History (password reuse) • Minimum password age • Password must meet complexity requirements Administrative access is restricted to user accounts accessible by authorized IT personnel.
164.312 (a)(2)(i)	**Unique user identification:** Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit and other related business functions.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • Expiration interval • History (password reuse) • Minimum password age • Password must meet complexity requirements
164.312 (a)(2)(ii)	**Emergency access procedure:** Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business recovery plans are tested periodically.
164.312 (a)(2)(iii)	**Automatic logoff:** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Workstations are configured to terminate inactive sessions after a period of inactivity. Users are required to re-validate with a username and password to gain control of the workstation.
164.312 (a)(2)(iv)	**Encryption and decryption:** Implement a mechanism to encrypt and decrypt ePHI.	SSL encryption technology is used for defined points of connectivity and data transmission.
164.312 (b)	**Audit controls:** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.

TECHNICAL SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
		Documented incident response policies and procedures are in place to guide personnel in the event of an incident. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
164.312 (c)(1)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	Documented shredding and destruction certificates from third party vendors are obtained and reviewed by management. System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • Expiration interval • History (password reuse) • Minimum password age • Password must meet complexity requirements SSL encryption technology is used for defined points of connectivity and data transmission.
164.312 (c)(2)	**Mechanisms to authenticate ePHI:** Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	SSL encryption technology is used for defined points of connectivity and data transmission.
164.312 (d)	**Person or entity authentication:** Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	System users are authenticated via individually-assigned user account and passwords. Production systems are configured to enforce password requirements that include: • Minimum length • Expiration interval • History (password reuse) • Minimum password age • Password must meet complexity requirements
164.312 (e)(1)	**Transmission security:** Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	SSL encryption technology is used for defined points of connectivity and data transmission.
164.312 (e)(2)(i)	**Integrity controls:** Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	SSL encryption technology is used for defined points of connectivity and data transmission.
164.312 (e)(2)(ii)	**Encryption:** Implement a mechanism to encrypt ePHI whenever deemed appropriate.	SSL encryption technology is used for defined points of connectivity and data transmission.

ORGANIZATIONAL SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.314 (a)(1)	**Business associate contracts or other arrangements:** A covered entity is not in compliance with the standards in § 164.502(e) if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful - (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary."	GRM maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.314 (a)(2)(i)	**Business Associate Contracts:** A business associate contract must provide that the business associate will: "Implement safeguards that protect the confidentiality, integrity, and availability of the electronic protected health; Report to the covered entity any security incident of which it becomes aware; Authorize termination of the contract, if the covered entity determines that the business associate has violated a material term of the contract."	GRM maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.314 (a)(2)(ii)	**Other Arrangement:** The Other Arrangements implementation specifications provide that when a covered entity and its business associate are both government entities, the covered entity may comply with the standard in either of two alternative ways.	**Not Applicable -** GRM is not a government entity.
164.314 (b)(1)	**Requirements for Group Health Plans:** Except when the only ePHI disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	**Not Applicable** - GRM is not a plan sponsor.

ORGANIZATIONAL SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.314 (b)(2)	**Implementation Specifications:** The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.	**Not Applicable** - GRM is not a plan sponsor.
164.316 (a)	**Policies and Procedures:** Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in 164.306(b)(2)(i), (ii), (iii), and (iv) [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard.	GRM creates and implements appropriate policies and procedures as required by law and as suggested by good business practices and general business ethics. Policies and procedures are reviewed and updated, if necessary; distributed, or otherwise made available to personnel; and are regularly maintained and secured.
164.316 (b)(1)	**Documentation:** Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Documentation is created and maintained in written and electronic form. Actions, activities, or assessments that arise from HIPAA related events are documented in the ticketing system.
164.316 (b)(1)(i)	**Time Limit:** Retain the documentation required by paragraph (b) (1) of this section for 6 years for the date of its creation or the date when it last was in effect, whichever is later.	GRM retains all documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect.
164.316 (b)(1)(ii)	**Availability:** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	HIPAA - related documentation is distributed or made otherwise available to all workforce members.
164.316 (b)(1)(iii)	**Updates:** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Documentation is reviewed annually and updated as needed in response to environmental or operation changes affecting the privacy or security of individually identifiable health information.

BREACH SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.402	Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (b)	Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 days after discovery of a breach.	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (c)(1)	Elements of the notification required by paragraph (a) of this section shall include to the extent possible: (A)a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) a description of the types of unsecured protected health information that were involved in the breach (Such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (C) any steps the individual should take to protect themselves from potential harm resulting from the breach;	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
	(D) a brief description of what the covered entity is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches; and (E) contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an email address, website, or postal address.	
164.404 (c)(2)	The notification required by paragraph (a) of this section shall be written in plain language.	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(1)(i)	The notification required by paragraph (a) shall be provided in the following form: Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available.	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(1)(ii)	The notification required by paragraph (a) shall be provided in the following form: If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)	**Substitute notice.** In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonable calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)(i)	In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means.	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.404 (d)(2)(ii)	In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(3)	In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.406	§164.406(a) For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. (b)Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. (c) The content of the notification required by paragraph (a) shall meet the requirements of §164.404(c).	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (b)	For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, expect as provided in §164.412, provide the notification required by paragraph (a) contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site.	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH SAFEGUARD		
Control Point	**Requirement**	**Control Activity Specified by the Service Organization**
164.408 (c)	For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calandar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.	GRM is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.410 (a)(1)	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	Breach notification policy and procedures are in place to be used during a breach of ePHI.
164.410 (a)(2)	(2) For the purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).	GRM acknowledges rasponsibility for notifying affected parties in the event of a breach of unsecured protected health information.
164.410 (b)	Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.	GRM notifies affected parties of a breach of ePHI no later than sixty (60) calendar days after the discovery of the breach.
164.410 (c)(1)	The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, used or disclosure during the breach.	The identification of each individual whose unsecured ePHI has been accessed during the breach is disclosed during notification procedures.
164.410 (c)(2)	A business associate shall provide the covered entity with any other information that the covered entity is required to include in the notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	Management provides the covered entity with any information that the covered entity is required to include in the notification to the individual at the time of the breach and as soon as it is available.

BREACH SAFEGUARD		
Control Point	**Control Point**	**Control Point**
164.412	If a law enforcement official states to a covered entity or business associate that a notification, notice or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies tha time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longar than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	GRM refrains from, or delays notifying the covered entity, or other required persons following the discovery of a breach of unsecured protected health information when required by law.
164.414	**Administrative requirements and burden of proof**: In the event of a use or disclosure in violation of subpart E, the covered entity or business associate; as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402. See §164.530 for definition of breach.	GRM acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protacted health information.

MONITORING

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. GRM's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

GRM's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in GRM's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of GRM's personnel.

Reporting Deficiencies

Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked. Management meetings are held to review reported deficiencies and corrective actions.

Policies and Procedures

Information security policies and procedures have been implemented regarding the protection of information assets. The policies and procedures act as a guide for all GRM personnel. These policies and procedures define guidelines for the information security program related to scope of services, which includes implementing and managing logical access security and controls, including the following:

- Information security policy
- Asset management
- Data classification
- Business continuity
- Incident management
- Access control
- Physical security

These policies are reviewed and approved by management on at least an annual basis.

Security Awareness Training

GRM security policies are documented and available to employees. Employees receive security awareness training for information security as part of the onboarding process. This training is reinforced by security awareness communications on current issues which are distributed periodically. Additionally, employees are also required to participate in annual security awareness training.

Periodic Testing and Evaluation

GRM completes evaluations throughout each calendar year regarding the effectiveness of the information security program that include, but are not limited to, the following:

- Internal risk assessments
- Corrective action plans
- Management reviews

Remediation and Continuous Improvement

Areas of non-compliance in GRM's internal control system surface from many sources, including the Company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings, if identified, of internal control non-compliant items should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to areas of non-compliance in internal control procedures and make the decision for addressing any non-compliant items based on whether the incident was isolated or requires a change in the Company's procedures or personnel.

Incident Response

GRM maintains a documented incident response plan including breach notification requirements as mandated by HITECH. The procedures include, but are not limited to, the identification, response, escalation, and remediation of security breaches and other incidents. A formal breach notification process is utilized to document and track resolution of incidents noted. The incident response procedures are tested during the normal course of business and are updated as needed.

COMPLEMENTARY USER ENTITY CONTROLS

GRM's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all requirements related to GRM's services to be solely achieved by GRM control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of GRM's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the requirements described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to GRM.
2. User entities are responsible for notifying GRM of changes made to technical or administrative contact information.
3. User entities are responsible for ensuring the supervision, management and control of the use of GRM services by their personnel.
4. User entities and subservice organizations are responsible for understanding and complying with their contractual obligations to GRM.
5. User entities are responsible for notifying GRM of changes made to technical or administrative contact information.
6. User entities are responsible for maintaining their own system(s) of record.
7. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize GRM services.
8. User entities are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals.
9. User entities are responsible for ensuring the confidentiality of any user IDs and passwords used to access GRM's systems.

VisualVault Support for HIPAA Compliance

HIPAA Requirement	Regulation	VisualVault
Risk Management	164.308 (a)(1)(ii)	Audit logs and log archival allow risk analysis and reduction.
Timely reports available to identify risks and potential concerns	• Risk Analysis	
	• Risk Management	
Access Management	164.308 (a)(4)(ii)(B,C)	VisualVault supports access management with access controls limiting user access. Detailed audit and access logging track login/logout, form field changes, form creation, form deletion, document creation or edits, document viewing, document deletion, and document purge. Authorized user access provides transparent data decryption (all data encrypted in transit and at rest). Configurable session timeout provides automatic logoff.
Provide authorization of access to users, authentication and de-registration of users when appropriate	164.308 (a)(5)(ii)(C)	
	164.312 (a)(2)(i)	
	164.312 (a)(2),ii)	
	164.312 (a)(2),iii)	
	164.312(c)(1,2)	
	• Access Authorization,	
	Establishment, Modification	
	• Login Monitoring	
	• Unique User ID	
	• Emergency Access Procedure	
	• Automatic logoff	
	• Integrity and authenticity	
	of ePHI	

Encryption and Decryption	164.312 (a)(2)(iv)	VisualVault encrypts data in transit (using TLS 1.2 or higher) and data at rest. Data at rest encryption process and policy can be found in: *VisualVault Encryption and Key Management.pdf*
While not specifically required by HIPAA, some organizations require that data be encrypted to meet certain standards. Some organizations provide "safe harbor" to their partners when data remains in the encrypted state.	164.312 (e)(2)(ii)	
	164.312(e)(2)(i)	
	164.312(c)(2)	
	• Encryption and	
	Decryption	
	• Encryption	
	• Integrity	
	• Mechanism to Authenticate	
	electronic health information	
Key management	164.312 (a)(2)(iv)	VisualVault's key management policy relies on Hardened Security Appliances (HAS) provided by Amazon's Key Management Service (KMS). VisualVault encryption key management policy can be found in: *VisualVault Encryption and Key Management.pdf*
Effective Key management and protection must be demonstrated to support the encrypted state of data.	164.312 (e)(2)(i)	
	• Encryption and Decryption	
	• Integrity Controls	
Logging – Audit Controls	164.312 (b)	VisualVault provides detailed audit and access logging track login/logout, form field changes, form creation, form deletion, document creation or edits, document viewing, document deletion, and document purge. Logs are archived and retained in a database.
Audit trails of access to data must be created and maintained.	• Audit Controls	
Monitoring	164.308 (a)(1)(ii)(D)	Access to PHI data is controlled by assigning

Organizations are required to ensure that access to PHI/PII data is appropriate.	• Information System Activity	groups permissions to view or modify data then assigning users to those groups. Upon initial user creation, the user account has access to no data and must be added to the appropriate groups by an administer or by an automated provisioning process established in advance.
Security Incident management	164.308 (a)(6)(ii) • Response and Reporting	VisualVault stores the most recent 2 weeks of system logs in a log management system with alerts to notify administrators of unusual activity. Log data older than 2 weeks is archived in a database and available for searching or analysis. Intrusion detection system with centralized management console is deployed on all VisualVault server nodes. A formal security incident response plan can be found in: *ISO - 0040 Information Security Incident Response Plan.pdf*
DR and Data Backup	164.308 (a)(7)(i) • Contingency Plan	VisualVault's cloud hosting environment consists of redundant systems located in two data centers with automatic failover at multiple system levels including web server failover, database node failover, application server node failover, and complete data center failover. Additionally, customer data is replicated to a geographically separated data center location. DR and Data Backup plan/procedures are documented in: *ISO-0015 VisualVault Disaster Recover and Business Continuity Plan.pdf,* *GRM VisualVault SOP-0009 Data Retention Backup and Restore.pdf*

VisualVault Technical Summary

Table of Contents

ıtroduction

VisualVault is a platform for building document and data intensive business processes. The architecture features an easily accessible API using industry standard authentication protocols combined with a micro services library allowing for rapid application development.

Overall system architecture is designed to utilize distributed computing resources by separating key system components into modular units which may be deployed across multiple server nodes. A single instance of the application consists of user interface (web servers), background tasks (application servers), document indexing, document searching, and data storage components.

Identity and Access Control Protocols

VisualVault supports different protocol options for Authentication and Authorization based on the specific use case required.

OAuth2

Used for Authentication and Authorization with the VisualVault REST (HTTP) APIs and support common security flows such as those for web server, installed, and client-side applications.

`AML2 (Single Sign-On)

VisualVault supports Single Sign-on using the SAML2 protocol allowing users to authenticate seamlessly using their organization's credentials.

LDAP

VisualVault 4 will continue to support LDAP synchronization and authentication using SSL for backwards compatibility. However, Federated Identity using the SAML2 protocol is now the preferred single sign-on configuration.

Local Accounts

Local accounts rely only on a User Id and stored password hash value for authentication. The accounts are created directly within VisualVault's user admin screen (or the Central Admin UI).

VisualVault local accounts support User Id expiration, password expiration, and complex password rule requirements. If an external identity provider is used the account and password rules must be implemented by the identity provider.

Data Encryption

- All client communications use HTTPS with a 2048-bit RSA key
- Data at rest encryption relies on Hardware Security Modules (HSMs) for encryption key management and multi-factor encryption:

- Each file is encrypted using multi-factor encryption (two encryption keys)
- Files data is encrypted using AES-256
- Each file has a unique AES encryption key
- Master key is used to encrypt each file's AES encryption key
- Master keys are managed by a Hardware Security Module

Compliance Standards

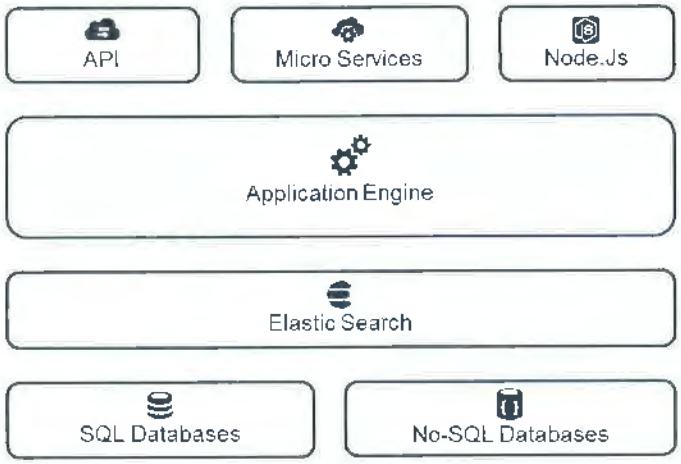
Cloud Data Protection	Annual SOC2 audit HIPAA HITECH (3rd party assessment)
Data Centers	SOC2
Record Centers	SOC2
Scanning Centers	SOC2
Document Imaging	SOC2, HIPAA HITECH
Medical Records	SOC2, HIPAA HITECH
Software Engineering	SOC2

Policies and Procedures

The following policies and procedures are available for review upon request

- SOC 2 Type 2 examination (3rd party assessment)
- HIPPA-HITECH Security Assessment (3rd party assessment)
- Disaster recovery and business continuity plan
- Network Architecture Diagram
- Support SLA
- SOP-0008 Configuration Management
- SOP-0006 Software Development Life Cycle
- SOP-0003 Change Control
- SOP-0009 Data Retention Backup and Restore
- STD-0001 IT Security Standard
- ISO-0036 Security in Development and Support Processes
- SOP-0010 Software coding standards
- Annual third-party penetration test
- Encryption and Key Management Procedure
- ISO-0039 Information Security Incident Management
- ISO-0040 Information Security Incident Response Plan
- Routine internal vulnerability scans

ıtegration



REST API

Platform & language neutral API which can be used to import data, submit electronic form records, upload files, attach or relate files and forms, create/edit users and groups, search forms and documents, download files. The API could be used to auto reconcile agent records with an external system on a scheduled basis.

'icro Services Library

VisualVault micro services library supports Node.Js scripts or web service end points. Node.Js scripts and web services can interact with VisualVault APIs as well as external system's APIs including any of Citizen's other system which provide API accessibility.

Micro Services Scheduler

VisualVault micro services can be scheduled to import / export data using VisualVault APIs and external system APIs.

Data Connections Library

VisualVault provides a data connections library designed to allow direct data queries against Oracle or Microsoft SQL Server databases via Web Services. The data connections library is commonly used by the intelligent forms to populate form drop down lists, document index field drop down lists, or auto-populate form fields as a user is filling out a form. Additionally, the VisualVault API can access the data connections allowing a micro service to query data and use it for validation of business rules.

System Feature Summary

The following is a brief overview of the primary system features intended to provide context to the rest of the document. For full system feature details refer to the Software Requirements Specification and the ıline help guide.

'ulti-Tenant

VisualVault is a multi-tenant capable architecture with centralized administration. Tenant and configuration data is stored in a configuration database with customer content stored in segregated content databases (or optional partitioned databases). Optional dedicated instances are available for a fee.

Central Admin

The Central Administration user interface components provide management and oversight of all Customers (tenants), user accounts, databases, servers, background tasks, logging, and configuration settings.

Intelligent Forms

VisualVault Forms provides a drag and drop form design tool that allows you to setup simple or complex forms without any coding. You can design a form template that intuitively prompts a person to enter data in a way that drives an intelligent business process. When a person fills in and saves a form, a form record is created. Interactive Form Dashboards are used to manage form processes.

When form process requirements are limited by out of the box functionality, you can extend the form processes using JavaScript (integrated script editor/library) and the JavaScript/REST APIs. Also available for process extensibility is the ability to define and interact with outside services including SOAP-based web services and server-side Node.Js scripts.

Other form features Include:

- Show relevant form fields or text based upon user inputs using the conditional form features within the designer.
- Control when form fields are visible and when they are read only based upon when a user is in a group or when data on the form is in a certain state.
- Upload documents, automatically route the documents to folders based on static or dynamic folder path rules.
- Use data from other database sources or forms to auto-populate fields.
- Create and display sub forms that drive different workflows from a parent form.
- Complete workflow tasks in the form interface using buttons or signature stamps.
- Outside services or JavaScript may be used to validate and complete custom actions on the form.
- Actions may include messaging, error flags, field population, etc.

Form templates, after design is completed, are released for users to begin filling in and capturing information. As a business process changes or the need to capture additional information arises; owners and administrators can quickly create a new revision of the form to capture new information immediately.

Document Management

GRM VisualVault allows the organization of documents into multiple level folder structures. The ›cument library is secured by assigning groups or users Folder permissions. If a user has not been granted rights to a Folder they will not see that Folder exists.

Administrators can apply security, define Index Fields (user defined fields), create retention rules, and define workflow templates for each Folder.

Index Fields definitions are available to all Folders within a Customer Vault and are managed centrally. Not all index fields are relevant to every type of document; folder level index field associations define which fields are available for use for the documents belonging to the folder

Each document uploaded to a Vault has an "ID card" where all document specific data is managed including revision history, active and historic workflows, security assignments, relationships to documents, forms, and projects, and history log (audit trail).

Folder level workflow templates may be defined such that new or modified documents trigger pre-defined or conditional workflow that helps control the life cycle of the document.

Workflow

The workflow engine is tightly integrated with folders, documents and forms. It provides capabilities to route documents or forms through a business process so the right individuals can perform work that is traceable. Workflows can be static or dynamic using conditional logic.

Reporting

Visibility and trending of your business processes are important. As a result, there are various methods report on and display information captured in VisualVault.

- End-user report writer
- Document lists can show index field data (user defined field data) using "custom views"
- Search results can be configured to display a specific "custom view" which includes index field and system columns.
- An optional third-party report server can be utilized to report on document information, security, revisions, etc.
- Interactive form dashboards can act as detailed reporting of form records.
- Form dashboards can display data from a single form template's records and may also be configured to join data from another form or data source.
- An interactive workflow report provides visibility of active workflows for any form or document that the user has permission to access.
- Training log – shows the list of document/form training that is required along with the status.
- Customizable home screens and menus may be used to display form dashboards and document lists using pre-defined or dynamic filters.

Configurable Roles

Configurable roles allow mapping system privileges and user accounts to named roles. Roles are essentially used to group system privileges and user accounts.

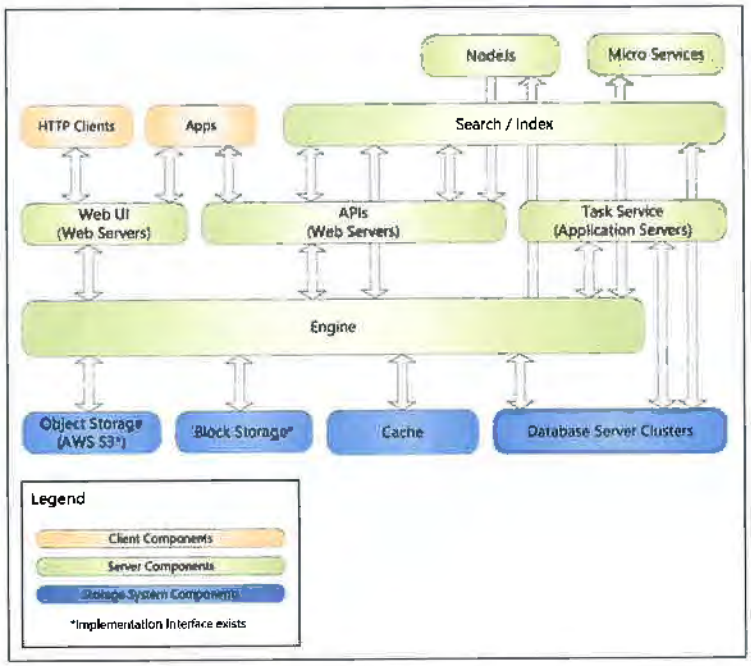
GRM VisualVault supports three configurable named roles sets: Owner, Editor, and Viewer. These permission sets each encapsulate a specific set of permissions used to grant a User or Group access to resources stored in a content database.

ogical Architecture

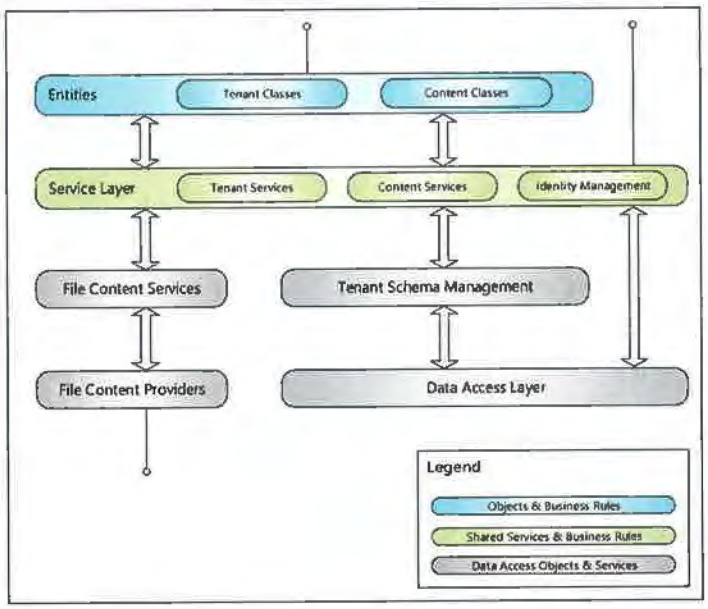
Application Engine

The User Interface (web servers), API, and application server components are each dependent upon the VisualVault Engine. Other system components interface with the Engine primarily through API calls.

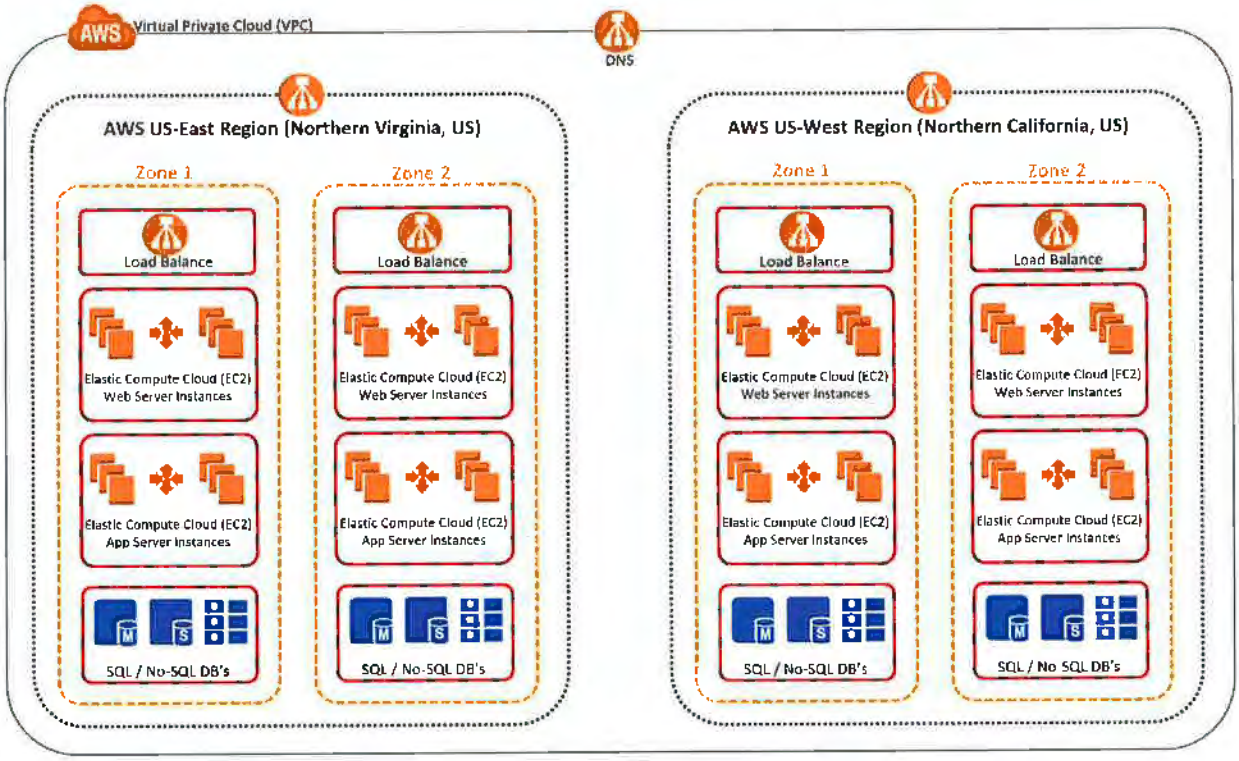
System Component Data Flow



Application Engine Data Flow



hysical Architecture



DISASTER RECOVERY and BUSINESS CONTINUITY PLAN

Last modified: December 28th 2016

TABLE OF CONTENTS

1 Plan Introduction

A comprehensive disaster recovery plan has been established to ensure continuity of operations for VisualVault during natural and man-made disasters.

This document serves as both a summary and a guide for actions to take during a disaster. Some action items reference related documents noted in section 1.3 and called out within specific recovery plan action items.

1.1 Responding to Disaster or Business Interruption

If you are responding to a disaster scenario go to Section 4, Recovery Strategy.

1.2 Definitions

Disaster is any interruption to operations that prompts a decision to execute a disaster recovery plan option.

Recovery Time Objective (RTO) is the target period of time by which a business service must be restored after a disaster or service disruption.

Recovery Point Objective (RPO) is the maximum acceptable period of data loss caused by a disaster or service disruption.

Cloud Computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the Internet.

Amazon Web Services (AWS) is a secure cloud computing platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow.

Amazon Elastic Compute Cloud (EC2) is a set of AWS services that provide scalable computing capacity within the Amazon Web Services (AWS) cloud. EC2 allows customers to launch virtual servers (EC2 instances) as needed, configure security and networking, and manage storage.

AWS Virtual Private Cloud (VPC) is a virtual network logically isolated from other virtual networks in the AWS cloud. AWS resources, such as Amazon EC2 instances,

are launched within a VPC. Each VPC has a configurable IP address range and can contain subnets, route tables, network gateways, and firewall rules.

AWS Regions and Availability Zones (AZs) Amazon EC2 is hosted in multiple locations world-wide. These locations are composed of regions and Availability Zones. Each *region* is a separate geographic area. Each region has multiple, isolated data center locations known as *Availability Zones*. Amazon EC2 provides the ability to place resources, such as instances, and data in multiple locations. Resources can be replicated across regions.

Amazon Simple Storage Service (S3) is a secure object storage service used to store and retrieve any amount of data. S3 is designed to deliver 99.999999999% durability, and scale past trillions of objects worldwide. S3 is used as a bulk repository for analytics, backup & recovery, disaster recovery, and primary storage for many cloud-native applications.

Primary and Backup Data Center Locations (PDC1, PDC2) (BDC1, BDC2)
VisualVault infrastructure utilizes two AWS primary data centers (PDC1 and PDC2) and two AWS backup data centers (BDC1 and BDC2). PDC1 and PDC2 are separate Availability Zones (data centers) located in Amazon's Northern Virginia Region; BDC1 and BDC2 are separate Availability Zones located in Amazon's Northern California Region.

1.3 Related Documents

- Network Architecture Diagram
- AWS Data Center Warm Startup work instruction
  - This work instruction is referenced by recovery plans 3,4,8 and 9
  - This work instruction defines the actions required to power on pre-configured EC2 instances, attach EBS volumes, initiate database restoration when necessary, and modify public DNS records (when necessary) when recovering from complete data center interruption.
- AWS Cold Data Center Startup work instruction
  - This work instruction is referenced by recovery plans 10
  - This work instruction defines the actions required to create a new AWS VPC using Amazon Machine Image (AMI) backups when recovering from the complete interruption of an AWS Region.

1.4 Mission and Objectives

The Disaster Recovery Plan (DRP) establishes defined responsibilities, actions and procedures to recover the VisualVault SaaS Infrastructure and data in the event of an unexpected interruption. The plan is structured to attain the following objectives:

(1) Recover network, computer systems, and software services within the Critical Time Frames established and defined in section 2.2

(2) Minimize the impact on business operations

1.5 Scope

The scope of the plan is to recover network, computer systems, software and business services at multiple data center locations referenced as Primary Data Center 1 (PDC1), Primary Data Center 2 (PDC2), Backup Data Center 1 (BDC1), and Backup Data Center 2 (BDC2).

1.6 Authorization

The management of VisualVault recognizes the need for a Disaster Recovery Plan for all operations directly or indirectly dependent on Software as a Service (SaaS) operations.

The Disaster Recovery Plan and Process has been reviewed and approved by senior management.

1.7 Responsibility

Responsibility for the development and maintenance of the plan is assumed by the Disaster Recovery team (see section 8.3).

1.8 Key Plan Assumptions

The following assumptions have been established as the basis for the development of the Disaster Recovery Plan:

This plan is designed to recover from a disruption or destruction of up to four data centers (PDC1, PDC2, BDC1, BDC2) located in two geographic regions (PDC and BDC regions) within the recovery time objectives stated in section 2.2.

This plan also has a contingency for the complete disruption of both the PDC and BDC regions which relies on the availability of an AWS Region outside of North America.

This plan is documented to the extent that an employee (or contractor if so authorized) can assume the key management role in the execution of the plan.

Although this plan is designed for worst case, inherent in the plan strategy is the ability to recover up to the most minor interruption, which is perhaps a more likely situation.

The plan is based on enough center staff being available to implement and affect recovery. The level of detail in the plan is written to staff experienced in the company's software delivery services.

2 Business Impact Analysis

2.1 SaaS and Business Services

This section of the plan defines each critical SaaS or business service and identifies the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for all critical services.

Note: Section 2.2 provides the RTO & RPO summary matrix for all services.

2.1.1 Primary Data Center 1 (PDC1)

2.1.1.1 PDC1 Components

- Firewall security groups
- Load balancing virtual appliances (redundant with failover)
- Multiple load balanced Web servers (redundant with failover)
- Redundant Database servers (redundant with failover)
- Backup software and services
- Management servers
- VisualVault application components
- FTP servers
- AWS Services
  - S3
  - EC2
  - DNS (Route 53)

2.1.2 Primary Data Center 2 (PDC2)

2.1.2.1 PDC2 Components

- Firewall security groups
- Load balancing virtual appliances (redundant with failover)
- Multiple load balanced Web servers (redundant with failover)

- Redundant Database servers (redundant with failover)
- Backup software and services
- Management servers
- VisualVault application components
- FTP servers
- AWS Services
  - S3
  - EC2
  - DNS (Route 53)

2.1.3 Backup Data Center 1 (BDC1)

2.1.3.1 BDC1 Components

- Firewall security groups
- Load balancing virtual appliances (redundant with failover) *
- Multiple load balanced Web servers (redundant with failover) *
- Redundant Database servers (redundant with failover) *
- Backup software and services
- Management servers *
- VisualVault application servers *
  - Web
  - API
  - Task
- FTP servers *
- AWS Services
  - S3
  - EC2
  - DNS (Route 53)

*servers are configured and ready for use but only powered on periodically for maintenance or in the case of implementing a recovery plan

2.1.4 Backup Data Center 2 (BDC2)

2.1.4.1 BDC1 Components

- Firewall security groups
- Load balancing virtual appliances (redundant with failover) *
- Multiple load balanced Web servers (redundant with failover) *
- Redundant Database servers (redundant with failover) *
- Backup software and services
- Management servers *
- VisualVault application servers *
  - Web
  - API
  - Task
- FTP servers *
- AWS Services
  - S3
  - EC2
  - DNS (Route 53)

*servers are configured and ready for use but only powered on periodically for maintenance or in the case of implementing a recovery plan

2.1.5 Support Software Systems

2.1.5.1 Support Software Systems Components

- Service Cloud (provided by SalesForce.com) (SaaS)

- Gmail (provided by Google) (SaaS)

2.1.6 Email Systems

2.1.6.1 Email Systems Components

- Gmail (provided by Google) (SaaS)

2.1.7 Source Code Repository

2.1.7.1 Source Code Repository Components

- Team Foundation Server (TFS) application service
- Redundant Database servers (redundant with failover)
- Backup software and services
- AWS Services
  - EC2
  - DNS (Route 53)

2.1.8 Development Tools

2.1.8.1 Development Tools Components

- Visual Studio 2015 Enterprise Integrated Development Environment (installed on each engineering workstation computer).
- JetBrains Re-Sharper Software Extension for Visual Studio (installed on each engineering workstation computer).
- Engineering workstation computers

2.1.9 CRM Software Systems

2.1.9.1 CRM Software Systems Components

- SalesForce.com (SaaS)

2.1.10 Financial Software

2.1.10.1 Financial Software Systems Components

- Great Plains (hosted by m-management) (SaaS)

2.1.11 General Business Software

2.1.11.1 General Business Software Components

- Microsoft Office 2016 (all employee workstations)
- Visio 2016 (select employee workstations)
- Microsoft Project 2016 (select employee workstations)

2.2 Recovery Time Objective Matrix

Recovery Time Objective (RTO)	< 1 Hour	1-4 Hours	4-24 Hours	24-48 Hours	**Data Recovery Point Objective (RPO)**
Primary Data Center 1 (PDC1) Customer access to VisualVault services and customer data	X				30 minutes
Primary Data Center 2 (PDC2) Customer access to VisualVault services and customer data	X				30 minutes
Backup Data Center 1 (BDC1) Geographically separated replica of PDC1 data		X			30 minutes
Backup Data Center 2 (BDC2) Geographically separated replica of PDC2 data		X			30 minutes
Support Software Systems		X			20 minutes
Email		X			20 minutes
Source Code Repository			X		24 hours
Development Tools			X		24 hours
CRM				X	24 hours
Financial Software				X	24 hours
General Business Applications				X	24 hours

3 Backup Strategy

VisualVault relies on AWS services to backup customer data and uses geographic separation of data backups to minimize risk.

All customer data is encrypted at rest and replicated from a Primary Data Center to two other Data Center locations including at least one geographically separated Data Center location. Specific backup procedures and locations are detailed below.

Off-site backup archives (export from AWS S3 storage service to encrypted hard drives) are performed by customer request only and additional fees apply.

Backup and restore procedures are defined in document SOP-0009. A summary of the backup and restore procedures is included in section 3.1 for reference.

3.1 General Backup Strategy

1.1 SQL Database Backup Procedure

- SQL database files and log files are replicated (synchronous replication) between PDC1 and PDC2 data centers to facilitate auto-failover between the PDC1 and PDC2 data centers.
- SQL database servers are implemented using a cluster configuration with automatic fail-over between the PDC1 and PDC2 data centers.
- SQL log files are backed up to an AWS S3 bucket at 20 minute intervals using IDERA SQL Safe Backup software which automates and monitors backup processes. The backed up log files (located in an AWS S3 bucket) are replicated between the PDC and BDC geographical regions resulting in log file availability in the Backup Data Center region.
- SQL data files are backed up to an AWS S3 bucket nightly using IDERA SQL Safe Backup software which automates and monitors backup processes. The backed up data files (located in an AWS S3 bucket) are replicated between the PDC and BDC geographical regions resulting in data file availability in the Backup Data Center region.

3.1.2 Customer Files Backup Procedure

- Customer files are written by VisualVault directly to an AWS S3 bucket configured with S3 versioning and geographic replication.
- Each file version is maintained (never overwritten) including deleted files. File versions are only deleted when a file is purged within the VisualVault application recycle bin.
- AWS S3 stores each file in a minimum of three data center locations. Additionally, S3 buckets are configured to replicate all customer files between the PDC and BDC geographical regions resulting in customer file availability in the Backup Data Center region.
- Off-site archives (export from AWS to encrypted hard drives) are performed by customer request only and additional fees apply.

3.1.3 Server Image Backup Procedure

- Each VisualVault server configuration is saved as an Amazon Machine Image (AMI) and stored within an AWS S3 bucket. The S3 bucket holding the AMI files is replicated between the PDC and BDC geographical regions resulting in AMI file availability in the Backup Data Center region.

4 Recovery Strategy

The Recovery Strategy is based upon type of business interruption or disaster. Once the disaster type is determined follow the specified disaster recovery plan.

4.1 Identify the Disaster Scenario

Select the most appropriate disaster or business interruption scenario below and implement the designated recovery plan.

4.1.1 Primary Data Center 1 (PDC1) Partial Interruption

Implement Recovery Plan 1 when:

- PDC2 is operating normally
- PDC1 has a partial interruption of service which may include:
  - Load balancer offline or malfunctioning
  - Web server offline or malfunctioning
  - Task server offline or malfunctioning
  - API Web server offline or malfunctioning
  - Internal DNS server offline or malfunctioning
  - SQL database server offline or malfunctioning (includes SQL data or log EBS storage volumes)
  - AWS S3 Storage Service offline or malfunctioning

4.1.2 Primary Data Center 2 (PDC2) Partial Interruption

Implement Recovery Plan 2 when:

- PDC1 is operating normally
- PDC2 has a partial interruption of service which may include:
  - Load balancer offline or malfunctioning
  - Web server offline or malfunctioning
  - Task server offline or malfunctioning

- API Web server offline or malfunctioning
- Internal DNS server offline or malfunctioning
- SQL database server offline or malfunctioning (includes SQL data or log EBS storage volumes)
- AWS S3 Storage Service offline or malfunctioning

4.1.3 Primary Data Center 1 (PDC1) Complete Interruption

Implement Recovery Plan 3 when:

- PDC1 has a complete interruption of service
- PDC2 is operating normally

4.1.4 Primary Data Center 2 (PDC2) Complete Interruption

Implement Recovery Plan 4 when:

- PDC2 has a complete interruption of service
- PDC1 is operating normally

4.1.5 Primary Data Center Region (PDC Region) Complete Interruption

Implement Recovery Plan 5 when:

- PDC1 has a complete interruption of service
- PDC2 has a complete interruption of service

4.1.6 Backup Data Center 1 (BDC1) Partial Interruption

Implement Recovery Plan 6 when:

- PDC Region has a complete interruption of service
- BDC2 is operating normally
- BDC1 has a partial interruption of service which may include:

- Load balancer offline or malfunctioning
- Web server offline or malfunctioning
- Task server offline or malfunctioning
- API Web server offline or malfunctioning
- Internal DNS server offline or malfunctioning
- SQL database server offline or malfunctioning (includes SQL data or log EBS storage volumes)
- AWS S3 Storage Service offline or malfunctioning

4.1.7 Backup Data Center 2 (BDC2) Partial Interruption

Implement Recovery Plan 7 when:

- PDC Region has a complete interruption of service
- BDC1 is operating normally
- BDC2 has a partial interruption of service which may include:
  - Load balancer offline or malfunctioning
  - Web server offline or malfunctioning
  - Task server offline or malfunctioning
  - API Web server offline or malfunctioning
  - Internal DNS server offline or malfunctioning
  - SQL database server offline or malfunctioning (includes SQL data or log EBS storage volumes)
  - AWS S3 Storage Service offline or malfunctioning

4.1.8 Backup Data Center 1 (BDC1) Complete Interruption

Implement Recovery Plan 8 when:

- PDC Region has a complete interruption of service
- BDC1 has a complete interruption of service

- BDC2 is operating normally

4.1.9 Backup Data Center 2 (BDC2) Complete Interruption

Implement Recovery Plan 9 when:

- PDC Region has a complete interruption of service
- BDC2 has a complete interruption of service
- BDC1 is operating normally

4.1.10 Primary Data Center Region (PDC Region) and Backup Data Center Region (BDC Region) Complete Interruption

Implement Recovery Plan 10 when:

- PDC Region has a complete interruption of service
- BDC Region has a complete interruption of service

4.2 Recovery Plans

Refer to section 4.1 above to determine which recovery plan to follow.

4.2.1 Recovery Plan 1 – PDC1 Partial Interruption

Follow the steps below to correct a partial interruption of PDC1 services. This plan assumes the PDC2 data center is fully operational. Each PDC1 service is duplicated in the PDC2 data center and should fail over automatically when the corresponding PDC1 service is offline. However, a malfunctioning PDC1 service (vs. an offline service) can result in service interruption requiring manual action.

- Load balancer offline or malfunctioning
- Web server offline or malfunctioning
- API server offline or malfunctioning
- Task server offline or malfunctioning

- Internal DNS server offline or malfunctioning
- SQL database server offline or malfunctioning (includes SQL data or log EBS storage volumes)
- AWS S3 Storage Service offline or malfunctioning

4.2.1.1 Instructions by interruption type

4.2.1.1.1 Load balancer offline

This scenario refers to the KEMP Loadmaster http/https layer 7 load balancer device not the AWS Elastic Load Balancer service. This device is identified on the Network Diagram as "HTTPS Load Balancer" in the PDC1 data center.

If the load balancer is offline, the AWS Elastic Load Balancer service will detect this and automatically route traffic to the load balancer located in PDC2. This will result in no traffic flowing to the PDC1 Web or API servers (12.x subnet). There should be no service interruption to customers but additional load is placed on the PDC2 data center.

- Identify the load balancer offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image
- Submit corrective action form
- Submit change control form

4.2.1.1.2 Load balancer malfunction

This scenario refers to the KEMP Loadmaster http/https layer 7 load balancer device not the AWS Elastic Load Balancer service. This device is identified on the Network Diagram as "HTTPS Load Balancer"

If the load balancer is malfunctioning, the AWS Elastic Load Balancer service will NOT detect this and traffic will continue to be routed to the load balancer.

- Edit the AWS Elastic Load Balancer service configuration and temporarily disable the PDC1 load balancer. This will result in no traffic flowing to the PDC1 Web or API servers (12.x subnet).
- Identify the load balancer malfunction root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image

- Edit the AWS Elastic Load Balancer service configuration and enable the PDC1 load balancer allowing traffic to flow to the PDC1 Web or API servers (12.x subnet).
- Submit corrective action form
- Submit change control form

4.2.1.1.3 Web server offline

This scenario refers to the VisualVault application Web servers located in PDC1 subnet 12.x.

If a Web server is offline the http load balancer will detect this and automatically route traffic to alternate Web servers.

- Identify the Web server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.1.1.4 Web server malfunction

This scenario refers to the VisualVault application Web servers located in PDC1 subnet 12.x.

If a Web server is malfunctioning the http load balancer may NOT detect this and continue to route traffic to the malfunctioning Web server.

- Identify the Web server malfunction root cause.
- If the malfunction is isolated to a specific server, edit the http load balancer configuration and temporarily disable the malfunctioning server
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form
- If necessary, edit the http load balancer configuration and enable the server

4.2.1.1.5 API server offline

This scenario refers to the VisualVault application servers (API servers) located in PDC1 subnet 12.x.

If an API server is offline the http load balancer will detect this and automatically route traffic to alternate API servers.

- Identify the API server offline root cause

- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.1.1.6 API server malfunction

This scenario refers to the VisualVault application servers (API servers) located in PDC1 subnet 12.x

If an API server is malfunctioning the http load balancer may NOT detect this and continue to route traffic to the malfunctioning API server.

- Identify the API server malfunction root cause.
- If the malfunction is isolated to a specific server, edit the http load balancer configuration and temporarily disable the malfunctioning server
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form
- If necessary, edit the http load balancer configuration and enable the server

4.2.1.1.7 Task server offline

This scenario refers to the VisualVault background task servers located in PDC1 subnet 13.x.

If a Task server is offline an alternate Task server will process tasks.

- Identify the Task server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.1.1.8 Task server malfunction

This scenario refers to the VisualVault background task servers located in PDC1 subnet 13.x.

If a Task server is malfunctioning the server may continue processing tasks with errors. Root cause analysis should include a review of the Task service error logs, VisualVault error logs, and OS event logs.

- Identify the Task server malfunction root cause.

- If the malfunction is isolated to a specific server, stop the VisualVault task service to prevent further errors.
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form
- If necessary, re-start the VisualVault Task service

4.2.1.1.9 DNS server offline

This scenario refers to the DNS servers located in PDC1 subnet 11.x.

If a DNS server is offline an alternate DNS server will process DNS requests.

- Identify the DNS server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from update, etc.
- Submit corrective action form
- Submit change control form

4.2.1.1.10 DNS server malfunction

This scenario refers to the DNS servers located in PDC1 subnet 11.x.

If a DNS server is malfunctioning the server may continue to process requests and respond with outdated or incorrect responses.

- Identify the DNS server malfunction root cause.
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.1.1.11 SQL server offline

This scenario refers to the SQL servers located in PDC1 subnet 14.x.

SQL Servers are configured using a Windows Failover Cluster with a minimum of one database server node located in PDC1 and a minimum of one database server node located in PDC2.

SQL logs and data are replicated synchronously between then PDC1 and PDC2 data centers. Refer to section 3.1.1 SQL Database Backup Procedure for details.

4.2.1.1.11.1 SQL Server offline automated recovery actions

If a SQL server located in PDC1 goes offline the Failover Cluster configuration will automatically initiate one of the following actions:

- If the offline server was the "Active" cluster node:
  - SQL Server Services are moved to a healthy node
  - The healthy node may be located in PDC2 or PDC1
- If the offline server was not the "Active" cluster node:
  - The SQL Server Services on this node are marked as off-line and no longer eligible to be used for failover

4.2.1.1.11.2 SQL Server offline manual recovery actions

- Identify the SQL Server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from update, data repair, etc.
- Submit corrective action form
- Submit change control form

4.2.1.1.12 SQL server malfunction

This scenario refers to the SQL servers located in PDC1 subnet 14.x.

SQL Servers are configured using a Windows Failover Cluster with a minimum of one database server node located in PDC1 and a minimum of one database server node located in PDC2.

4.2.1.1.12.1 SQL Server malfunction automated recovery actions

If a SQL server located in PDC1 experiences a malfunction but continues to be viewed as online by the Failover Cluster, no automated action will be initiated.

4.2.1.1.12.2 SQL Server malfunction manual recovery actions

- Identify the SQL Server malfunction root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from update, data repair, etc.
- Submit corrective action form

- Submit change control form

4.2.2 Recovery Plan 2 - PDC2 Partial Interruption

Follow the steps below to correct a partial interruption of PDC2 services. This plan assumes the PDC1 data center is fully operational. Each PDC2 service is duplicated in the PDC1 data center and should fail over automatically when the corresponding PDC2 service is offline. However, a malfunctioning PDC2 service (vs. an offline service) can result in service interruption requiring manual action.

- Load balancer offline or malfunctioning
- Web server offline or malfunctioning
- API server offline or malfunctioning
- Task server offline or malfunctioning
- Internal DNS server offline or malfunctioning
- SQL database server offline or malfunctioning (includes SQL data or log EBS storage volumes)
- AWS S3 Storage Service offline or malfunctioning

4.2.2.1 Instructions by interruption type

4.2.2.1.1 Load balancer offline

This scenario refers to the KEMP Loadmaster http/https layer 7 load balancer device not the AWS Elastic Load Balancer service. This device is identified on the Network Diagram as "HTTPS Load Balancer" in the PDC2 data center.

If the load balancer is offline, the AWS Elastic Load Balancer service will detect this and automatically route traffic to the load balancer located in PDC1. This will result in no traffic flowing to the PDC2 Web or API servers (22.x subnet). There should be no service interruption to customers but additional load is placed on the PDC1 data center.

- Identify the load balancer offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image
- Submit corrective action form
- Submit change control form

4.2.2.1.2 Load balancer malfunction

This scenario refers to the KEMP Loadmaster http/https layer 7 load balancer device not the AWS Elastic Load Balancer service. This device is identified on the Network Diagram as "HTTPS Load Balancer" in the PDC2 data center.

If the load balancer is malfunctioning, the AWS Elastic Load Balancer service will NOT detect this and traffic will continue to be routed to the load balancer.

- Edit the AWS Elastic Load Balancer service configuration and temporarily disable the PDC2 load balancer. This will result in no traffic flowing to the PDC2 Web or API servers (22.x subnet).
- Identify the load balancer malfunction root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image
- Edit the AWS Elastic Load Balancer service configuration and enable the PDC2 load balancer allowing traffic to flow to the PDC2 Web or API servers (22.x subnet).
- Submit corrective action form
- Submit change control form

4.2.2.1.3 Web server offline

This scenario refers to the VisualVault application Web servers located in PDC2 subnet 22.x.

If a Web server is offline the http load balancer will detect this and automatically route traffic to alternate Web servers.

- Identify the Web server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.2.1.4 Web server malfunction

This scenario refers to the VisualVault application Web servers located in PDC2 subnet 22.x.

If a Web server is malfunctioning the http load balancer may NOT detect this and continue to route traffic to the malfunctioning Web server.

- Identify the Web server malfunction root cause.

- If the malfunction is isolated to a specific server, edit the http load balancer configuration and temporarily disable the malfunctioning server
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form
- If necessary, edit the http load balancer configuration and enable the server

4.2.2.1.5 API server offline

This scenario refers to the VisualVault application servers (API servers) located in PDC2 subnet 22.x.

If an API server is offline the http load balancer will detect this and automatically route traffic to alternate API servers.

- Identify the API server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.2.1.6 API server malfunction

This scenario refers to the VisualVault application servers (API servers) located in PDC2 subnet 22.x

If an API server is malfunctioning the http load balancer may NOT detect this and continue to route traffic to the malfunctioning API server.

- Identify the API server malfunction root cause.
- If the malfunction is isolated to a specific server, edit the http load balancer configuration and temporarily disable the malfunctioning server
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form
- If necessary, edit the http load balancer configuration and enable the server

4.2.2.1.7 Task server offline

This scenario refers to the VisualVault background task servers located in PDC2 subnet 23.x.

If a Task server is offline an alternate Task server will process tasks.

- Identify the Task server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.2.1.8 Task server malfunction

This scenario refers to the VisualVault background task servers located in PDC2 subnet 23.x.

If a Task server is malfunctioning the server may continue processing tasks with errors. Root cause analysis should include a review of the Task service error logs, VisualVault error logs, and OS event logs.

- Identify the Task server malfunction root cause.
- If the malfunction is isolated to a specific server, stop the VisualVault task service to prevent further errors.
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form
- If necessary, re-start the VisualVault Task service

4.2.2.1.9 DNS server offline

This scenario refers to the DNS servers located in PDC2 subnet 21.x.

If a DNS server is offline an alternate DNS server will process DNS requests.

- Identify the DNS server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from update, etc.
- Submit corrective action form
- Submit change control form

4.2.2.1.10 DNS server malfunction

This scenario refers to the DNS servers located in PDC2 subnet 21.x.

If a DNS server is malfunctioning the server may continue to process requests and respond with outdated or incorrect responses.

- Identify the DNS server malfunction root cause.
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.2.1.11 SQL server offline

This scenario refers to the SQL servers located in PDC2 subnet 24.x.

SQL Servers are configured using a Windows Failover Cluster with a minimum of one database server node located in PDC1 and a minimum of one database server node located in PDC2.

SQL logs and data are replicated synchronously between then PDC1 and PDC2 data centers. Refer to section 3.1.1 SQL Database Backup Procedure for details.

4.2.2.1.11.1 SQL Server offline automated recovery actions

If a SQL server located in PDC2 goes offline the Failover Cluster configuration will automatically initiate one of the following actions:

- If the offline server was the "Active" cluster node:
  - SQL Server Services are moved to a healthy node
  - The healthy node may be located in PDC2 or PDC1
- If the offline server was not the "Active" cluster node:
  - The SQL Server Services on this node are marked as off-line and no longer eligible to be used for failover

4.2.2.1.11.2 SQL Server offline manual recovery actions

- Identify the SQL Server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from update, data repair, etc.
- Submit corrective action form
- Submit change control form

4.2.2.1.12 SQL server malfunction

This scenario refers to the SQL servers located in PDC2 subnet 24.x.

SQL Servers are configured using a Windows Failover Cluster with a minimum of one database server node located in PDC1 and a minimum of one database server node located in PDC2.

4.2.2.1.12.1 SQL Server malfunction automated recovery actions

If a SQL server located in PDC2 experiences a malfunction but continues to be viewed as online by the Failover Cluster, no automated action will be initiated.

4.2.2.1.12.2 SQL Server malfunction manual recovery actions

- Identify the SQL Server malfunction root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from update, data repair, etc.
- Submit corrective action form
- Submit change control form

4.2.3 Recovery Plan 3 - PDC1 Complete Interruption

This plan assumes no services in the PDC1 data center are operational. This could be the result of a natural disaster, power and backup power system failure, HVAC system failure or any other cause resulting in a complete loss of services in the PDC1 data center.

This plan assumes the PDC2 data center is operational. If both the PDC1 and PDC2 data centers are not operational initiate Recovery Plan 5.

4.2.3.1.1.1 PDC1 complete interruption automated recovery actions

- Each PDC1 service is duplicated in the PDC2 data center. If the AWS Elastic Load Balance Service detects no response from the http load balancer located in PDC1 then all http/https traffic will be automatically redirected to the PDC2 data center.

4.2.3.1.1.2 PDC1 complete interruption manual recovery actions

- If the PDC1 complete interruption of service was caused by an AWS outage
  When AWS has restored service initiate the "AWS Data Center Warm Startup" Work Instruction. This work instruction defines the actions required to power on pre-configured EC2 instances, attach EBS volumes, initiate database restoration when necessary, and modify public DNS records (when necessary) when recovering from complete data center interruption.

4.2.4 Recovery Plan 4 - PDC2 Complete Interruption

This plan assumes no services in the PDC2 data center are operational. This could be the result of a natural disaster, power and backup power system failure, HVAC system failure or any other cause resulting in a complete loss of services in the PDC2 data center.

This plan assumes the PDC1 data center is operational. If both the PDC1 and PDC2 data centers are not operational initiate Recovery Plan 5.

4.2.4.1.1.1 PDC2 complete interruption automated recovery actions

- Each PDC2 service is duplicated in the PDC1 data center. If the AWS Elastic Load Balance Service detects no response from the http load balancer located in PDC2 then all http/https traffic will be automatically redirected to the PDC1 data center.

4.2.4.1.1.2 PDC2 complete interruption manual recovery actions

- If the PDC2 complete interruption of service was caused by an AWS outage
- When AWS has restored service initiate the "AWS Data Center Warm Startup" Work Instruction. This work instruction defines the actions required to power on pre-configured EC2 instances, attach EBS volumes, initiate database restoration when necessary, and modify public DNS records (when necessary) when recovering from complete data center interruption.

4.2.5 Recovery Plan 5 – PDC Region Complete Interruption

This plan assumes no services in the PDC data center region. This could be the result of a natural disaster, multiple power and backup power system failures, or any other cause resulting in a complete loss of services in the PDC data center region.

- All customer and database files are replicated (using Amazon S3 replication) to the Backup Data Center (BDC) region in order to meet the Recovery Point Objective (RPO).

- The BDC region has a minimal set of servers and services which are kept online continuously along with pre-configured EC2 instances which are periodically "powered on" to apply changes and patches.

- The BDC1 data center contains pre-configured EC2 instances which are a duplicate of all servers located in the PDC1 data center. Only a minimal number of EC2 instances are kept in a powered on state, refer to the Network Diagram document which shows typically powered down EC2 instances with a shaded background color.

- The BDC2 data center contains pre-configured EC2 instances which are a duplicate of all servers located in the PDC2 data center. Only a minimal number of EC2 instances are kept in a powered on state, refer to the Network Diagram document which shows typically powered down EC2 instances with a shaded background color.

- The BDC1 data center has a backup/restore server with EBS volumes attached which contain a copy of all database backup files from the prior 48 hours. The purpose of maintaining the most recent database backup files on an EBS volume is to reduce file transfer time from the Amazon S3 object storage service to the backup/restore server.

- Bring the PDC1 and PDC2 data centers online by following the "AWS Data Center Warm Startup" Work Instruction. This work instruction defines the actions required to power on pre-configured EC2 instances, attach EBS volumes, initiate database restoration when necessary, and modify public DNS records (when necessary) when recovering from complete data center interruption.

4.2.6 Recovery Plan 6 – BDC1 Partial Interruption

This plan assumes the Primary Data Center region (PDC Region) is offline and DNS records are directing all traffic to the Backup Data Center region. In this scenario, Recovery Plan 5 was previously implemented (both BDC1 and BDC2 data centers were brought online).

Follow the steps below to correct a partial interruption of BDC1 services. This plan assumes the BDC2 data center is fully operational. Each BDC1 service is duplicated in the BDC2 data center and should fail over automatically when the corresponding BDC1 service is offline. However, a malfunctioning BDC1 service (vs. an offline service) can result in service interruption requiring manual action.

- Load balancer offline or malfunctioning
- Web server offline or malfunctioning
- API server offline or malfunctioning
- Task server offline or malfunctioning
- Internal DNS server offline or malfunctioning
- SQL database server offline or malfunctioning (includes SQL data or log EBS storage volumes)
- AWS S3 Storage Service offline or malfunctioning

4.2.6.1 Instructions by interruption type

4.2.6.1.1 Load balancer offline

This scenario refers to the KEMP Loadmaster http/https layer 7 load balancer device not the AWS Elastic Load Balancer service. This device is identified on the Network Diagram as "HTTPS Load Balancer" in the BDC1 data center.

If the load balancer is offline, the AWS Elastic Load Balancer service will detect this and automatically route traffic to the load balancer located in BDC2. This will result in no traffic flowing to the BDC1 Web or API servers (52.x subnet). There should be no service interruption to customers but additional load is placed on the BDC2 data center.

- Identify the load balancer offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image
- Submit corrective action form

- Submit change control form

4.2.6.1.2 Load balancer malfunction

This scenario refers to the KEMP Loadmaster http/https layer 7 load balancer device not the AWS Elastic Load Balancer service. This device is identified on the Network Diagram as "HTTPS Load Balancer"

If the load balancer is malfunctioning, the AWS Elastic Load Balancer service will NOT detect this and traffic will continue to be routed to the load balancer.

- Edit the AWS Elastic Load Balancer service configuration and temporarily disable the BDC1 load balancer. This will result in no traffic flowing to the BDC1 Web or API servers (52.x subnet).
- Identify the load balancer malfunction root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image
- Edit the AWS Elastic Load Balancer service configuration and enable the BDC1 load balancer allowing traffic to flow to the BDC1 Web or API servers (52.x subnet).
- Submit corrective action form
- Submit change control form

4.2.6.1.3 Web server offline

This scenario refers to the VisualVault application Web servers located in BDC1 subnet 52.x.

If a Web server is offline the http load balancer will detect this and automatically route traffic to alternate Web servers.

- Identify the Web server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.6.1.4 Web server malfunction

This scenario refers to the VisualVault application Web servers located in BDC1 subnet 52.x.

If a Web server is malfunctioning the http load balancer may NOT detect this and continue to route traffic to the malfunctioning Web server.

- Identify the Web server malfunction root cause.
- If the malfunction is isolated to a specific server, edit the http load balancer configuration and temporarily disable the malfunctioning server
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form
- If necessary, edit the http load balancer configuration and enable the server

4.2.6.1.5 API server offline

This scenario refers to the VisualVault application servers (API servers) located in BDC1 subnet 52.x.

If an API server is offline the http load balancer will detect this and automatically route traffic to alternate API servers.

- Identify the API server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.6.1.6 API server malfunction

This scenario refers to the VisualVault application servers (API servers) located in BDC1 subnet 52.x

If an API server is malfunctioning the http load balancer may NOT detect this and continue to route traffic to the malfunctioning API server.

- Identify the API server malfunction root cause.
- If the malfunction is isolated to a specific server, edit the http load balancer configuration and temporarily disable the malfunctioning server
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form
- If necessary, edit the http load balancer configuration and enable the server

4.2.6.1.7 Task server offline

This scenario refers to the VisualVault background task servers located in BDC1 subnet 53.x.

If a Task server is offline an alternate Task server will process tasks.

- Identify the Task server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.6.1.8 Task server malfunction

This scenario refers to the VisualVault background task servers located in BDC1 subnet 53.x.

If a Task server is malfunctioning the server may continue processing tasks with errors. Root cause analysis should include a review of the Task service error logs, VisualVault error logs, and OS event logs.

- Identify the Task server malfunction root cause.
- If the malfunction is isolated to a specific server, stop the VisualVault task service to prevent further errors.
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form
- If necessary, re-start the VisualVault Task service

4.2.6.1.9 DNS server offline

This scenario refers to the DNS servers located in BDC1 subnet 51.x.

If a DNS server is offline an alternate DNS server will process DNS requests.

- Identify the DNS server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from update, etc.
- Submit corrective action form
- Submit change control form

4.2.6.1.10 DNS server malfunction

This scenario refers to the DNS servers located in BDC1 subnet 51.x.

If a DNS server is malfunctioning the server may continue to process requests and respond with outdated or incorrect responses.

- Identify the DNS server malfunction root cause.
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.6.1.11 SQL server offline

This scenario refers to the SQL servers located in BDC1 subnet 54.x.

SQL Servers are configured using a Windows Failover Cluster with a minimum of one database server node located in BDC1 and a minimum of one database server node located in BDC2.

SQL logs and data are replicated synchronously between then BDC1 and BDC2 data centers. `efer to section 3.1.1 SQL Database Backup Procedure for details.

4.2.6.1.11.1 SQL Server offline automated recovery actions

If a SQL server located in BDC1 goes offline the Failover Cluster configuration will automatically initiate one of the following actions:

- If the offline server was the "Active" cluster node:
  - SQL Server Services are moved to a healthy node
  - The healthy node may be located in BDC2 or BDC1
- If the offline server was not the "Active" cluster node:
  - The SQL Server Services on this node are marked as off-line and no longer eligible to be used for failover

4.2.6.1.11.2 SQL Server offline manual recovery actions

- Identify the SQL Server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from update, data repair, etc.
- Submit corrective action form
- Submit change control form

4.2.6.1.12 SQL server malfunction

This scenario refers to the SQL servers located in BDC1 subnet 54.x.

SQL Servers are configured using a Windows Failover Cluster with a minimum of one database server node located in BDC1 and a minimum of one database server node located in BDC2.

4.2.6.1.12.1 SQL Server malfunction automated recovery actions

If a SQL server located in BDC1 experiences a malfunction but continues to be viewed as online by the Failover Cluster, no automated action will be initiated.

4.2.6.1.12.2 SQL Server malfunction manual recovery actions

- Identify the SQL Server malfunction root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from update, data repair, etc.
- Submit corrective action form
- Submit change control form

4.2.7 Recovery Plan 7 – BDC2 Partial Interruption

This plan assumes the Primary Data Center region (PDC Region) is offline and DNS records are directing all traffic to the Backup Data Center region. In this scenario, Recovery Plan 5 was previously implemented (both BDC1 and BDC2 data centers were brought online).

Follow the steps below to correct a partial interruption of BDC2 services. This plan assumes the BDC1 data center is fully operational. Each BDC2 service is duplicated in the BDC1 data center and should fail over automatically when the corresponding BDC2 service is offline. However, a malfunctioning BDC2 service (vs. an offline service) can result in service interruption requiring manual action.

- Load balancer offline or malfunctioning
- Web server offline or malfunctioning
- API server offline or malfunctioning
- Task server offline or malfunctioning
- Internal DNS server offline or malfunctioning

- SQL database server offline or malfunctioning (includes SQL data or log EBS storage volumes)
- AWS S3 Storage Service offline or malfunctioning

4.2.7.1 Instructions by interruption type

4.2.7.1.1 Load balancer offline

This scenario refers to the KEMP Loadmaster http/https layer 7 load balancer device not the AWS Elastic Load Balancer service. This device is identified on the Network Diagram as "HTTPS Load Balancer" in the BDC2 data center.

If the load balancer is offline, the AWS Elastic Load Balancer service will detect this and automatically route traffic to the load balancer located in BDC1. This will result in no traffic flowing to the BDC2 Web or API servers (62.x subnet). There should be no service interruption to customers but additional load is placed on the BDC1 data center.

- Identify the load balancer offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image
- Submit corrective action form
- Submit change control form

4.2.7.1.2 Load balancer malfunction

This scenario refers to the KEMP Loadmaster http/https layer 7 load balancer device not the AWS Elastic Load Balancer service. This device is identified on the Network Diagram as "HTTPS Load Balancer" in the BDC2 data center.

If the load balancer is malfunctioning, the AWS Elastic Load Balancer service will NOT detect this and traffic will continue to be routed to the load balancer.

- Edit the AWS Elastic Load Balancer service configuration and temporarily disable the BDC2 load balancer. This will result in no traffic flowing to the BDC2 Web or API servers (62.x subnet).
- Identify the load balancer malfunction root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image
- Edit the AWS Elastic Load Balancer service configuration and enable the PDC2 load balancer allowing traffic to flow to the BDC2 Web or API servers (62.x subnet).

- Submit corrective action form
- Submit change control form

4.2.7.1.3 Web server offline

This scenario refers to the VisualVault application Web servers located in BDC2 subnet 62.x.

If a Web server is offline the http load balancer will detect this and automatically route traffic to alternate Web servers.

- Identify the Web server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.7.1.4 Web server malfunction

This scenario refers to the VisualVault application Web servers located in BDC2 subnet 62.x.

If a Web server is malfunctioning the http load balancer may NOT detect this and continue to route traffic to the malfunctioning Web server.

- Identify the Web server malfunction root cause.
- If the malfunction is isolated to a specific server, edit the http load balancer configuration and temporarily disable the malfunctioning server
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form
- If necessary, edit the http load balancer configuration and enable the server

4.2.7.1.5 API server offline

This scenario refers to the VisualVault application servers (API servers) located in BDC2 subnet 62.x.

If an API server is offline the http load balancer will detect this and automatically route traffic to alternate API servers.

- Identify the API server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form

- Submit change control form

4.2.7.1.6 API server malfunction

This scenario refers to the VisualVault application servers (API servers) located in BDC2 subnet 62.x

If an API server is malfunctioning the http load balancer may NOT detect this and continue to route traffic to the malfunctioning API server.

- Identify the API server malfunction root cause.
- If the malfunction is isolated to a specific server, edit the http load balancer configuration and temporarily disable the malfunctioning server
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form
- If necessary, edit the http load balancer configuration and enable the server

4.2.7.1.7 Task server offline

. nis scenario refers to the VisualVault background task servers located in BDC2 subnet 63.x.

If a Task server is offline an alternate Task server will process tasks.

- Identify the Task server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.7.1.8 Task server malfunction

This scenario refers to the VisualVault background task servers located in BDC2 subnet 63.x.

If a Task server is malfunctioning the server may continue processing tasks with errors. Root cause analysis should include a review of the Task service error logs, VisualVault error logs, and OS event logs.

- Identify the Task server malfunction root cause.
- If the malfunction is isolated to a specific server, stop the VisualVault task service to prevent further errors.

- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form
- If necessary, re-start the VisualVault Task service

4.2.7.1.9 DNS server offline

This scenario refers to the DNS servers located in BDC2 subnet 61.x.

If a DNS server is offline an alternate DNS server will process DNS requests.

- Identify the DNS server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from update, etc.
- Submit corrective action form
- Submit change control form

2.7.1.10 DNS server malfunction

This scenario refers to the DNS servers located in BDC2 subnet 61.x.

If a DNS server is malfunctioning the server may continue to process requests and respond with outdated or incorrect responses.

- Identify the DNS server malfunction root cause.
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from application update, etc.
- Submit corrective action form
- Submit change control form

4.2.7.1.11 SQL server offline

This scenario refers to the SQL servers located in BDC2 subnet 64.x.

SQL Servers are configured using a Windows Failover Cluster with a minimum of one database server node located in BDC1 and a minimum of one database server node located in BDC2.

SQL logs and data are replicated synchronously between then BDC1 and BDC2 data centers. Refer to section 3.1.1 SQL Database Backup Procedure for details.

4.2.7.1.11.1 SQL Server offline automated recovery actions

If a SQL server located in BDC2 goes offline the Failover Cluster configuration will automatically initiate one of the following actions:

- If the offline server was the "Active" cluster node:
  - SQL Server Services are moved to a healthy node
  - The healthy node may be located in BDC2 or BDC1
- If the offline server was not the "Active" cluster node:
  - The SQL Server Services on this node are marked as off-line and no longer eligible to be used for failover

4.2.7.1.11.2 SQL Server offline manual recovery actions

- Identify the SQL Server offline root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from update, data repair, etc.
- Submit corrective action form
- Submit change control form

4.2.7.1.12 SQL server malfunction

This scenario refers to the SQL servers located in BDC2 subnet 64.x.

SQL Servers are configured using a Windows Failover Cluster with a minimum of one database server node located in BDC1 and a minimum of one database server node located in BDC2.

4.2.7.1.12.1 SQL Server malfunction automated recovery actions

If a SQL server located in PDC2 experiences a malfunction but continues to be viewed as online by the Failover Cluster, no automated action will be initiated.

4.2.7.1.12.2 SQL Server malfunction manual recovery actions

- Identify the SQL Server malfunction root cause
- Implement corrective actions which may include restoring from a pre-saved Amazon Machine Image, rollback from update, data repair, etc.
- Submit corrective action form
- Submit change control form

4.2.8 Recovery Plan 8 – BDC1 Complete Interruption

This plan assumes the Primary Data Center region (PDC Region) is offline and DNS records are directing all traffic to the Backup Data Center region. In this scenario, Recovery Plan 5 was previously implemented (both BDC1 and BDC2 data centers were brought online).

This plan also assumes no services in the BDC1 data center are operational. This could be the result of a natural disaster, power and backup power system failure, HVAC system failure or any other cause resulting in a complete loss of services in the BDC1 data center.

This plan also assumes the BDC2 data center is operational. If both the BDC1 and BDC2 data centers are not operational initiate Recovery Plan 10.

..2.8.1.1.1 BDC1 complete interruption automated recovery actions

- Each BDC1 service is duplicated in the BDC2 data center. If the AWS Elastic Load Balance Service detects no response from the http load balancer located in BDC1 then all http/https traffic will be automatically redirected to the BDC2 data center.

4.2.8.1.1.2 BDC1 complete interruption manual recovery actions

- If the BDC1 complete interruption of service was caused by an AWS outage
- When AWS has restored service initiate work instruction "AWS Data Center Warm Startup". This work instruction defines the actions required to power on pre-configured EC2 instances, attach EBS volumes, initiate database restoration when necessary, and modify public DNS records (when necessary). when recovering from complete data center interruption.

4.2.9 Recovery Plan 9 - BDC2 Complete Interruption

This plan assumes the Primary Data Center region (PDC Region) is offline and DNS records are directing all traffic to the Backup Data Center region. In this scenario, Recovery Plan 5 was previously implemented (both BDC1 and BDC2 data centers were brought online).

This plan also assumes no services in the BDC2 data center are operational. This could be the result of a natural disaster, power and backup power system failure, HVAC system failure or any other cause resulting in a complete loss of services in the BDC2 data center.

This plan also assumes the BDC1 data center is operational. If both the BDC1 and BDC2 data centers are not operational initiate Recovery Plan 10.

4.2.9.1.1.1 BDC2 complete interruption automated recovery actions

- Each BDC2 service is duplicated in the BDC1 data center. If the AWS Elastic Load Balance Service detects no response from the http load balancer located in BDC2 then all http/https traffic will be automatically redirected to the BDC1 data center.

4.2.9.1.1.2 BDC2 complete interruption manual recovery actions

- If the BDC2 complete interruption of service was caused by an AWS outage
- When AWS has restored service initiate work instruction "AWS Data Center Warm Startup". This work instruction defines the actions required to power on pre-configured EC2 instances, attach EBS volumes, initiate database restoration when necessary, and modify public DNS records (when necessary) when recovering from complete data center interruption.

4.2.10 Recovery Plan 10 - Complete Interruption of PDC and BDC Regions

This plan assumes both the Primary and Backup Data Center regions (PDC and BDC Region) are offline.

4.2.10.1.1.1 PDC and BDC region complete interruption manual recovery actions

- If the PDC and BDC region complete interruption of service was caused by an AWS outage in the PDC/BDC regions.
    - Communicate with AWS representatives to get an estimated service restoration time.
    - If estimated service restoration time is less than the Recovery Time Objective (RTO) stated in section 2.2 then wait for AWS service restoration and communicate the estimated service restoration time to customers.
    - If estimated service restoration time is greater than the Recovery Time Objective (RTO) stated in section 2.2
        - Implement work instruction "AWS Data Center Cold Startup". This work instruction defines the actions required to create a new VPC using Amazon Machine Image (AMI) backups when recovering from a AWS region complete interruption.
        - Communicate with AWS representatives to determine the most appropriate AWS geographic region where the new VPC should be created.
        - Advise customers of the estimated Recovery Time Objective
- If the PDC and BDC region complete interruption of service was not caused by an AWS outage
    - Determine the root cause of the interruption
    - Determine the most appropriate recovery plan action items. For example, if the root cause is failure of all redundant load balance devices, follow the Load balancer offline or Load balancer malfunction recovery plan action items located in the most appropriate recovery plan.
    - Advise customers of the estimated Recovery Time Objective

5 Disaster Recovery Organization

The effectiveness and operability of the Disaster Recovery Plan is dependent on the knowledge and expertise of the personnel who develop and execute the plan. Skills and talents are required and to assign personnel who meet those requirements.

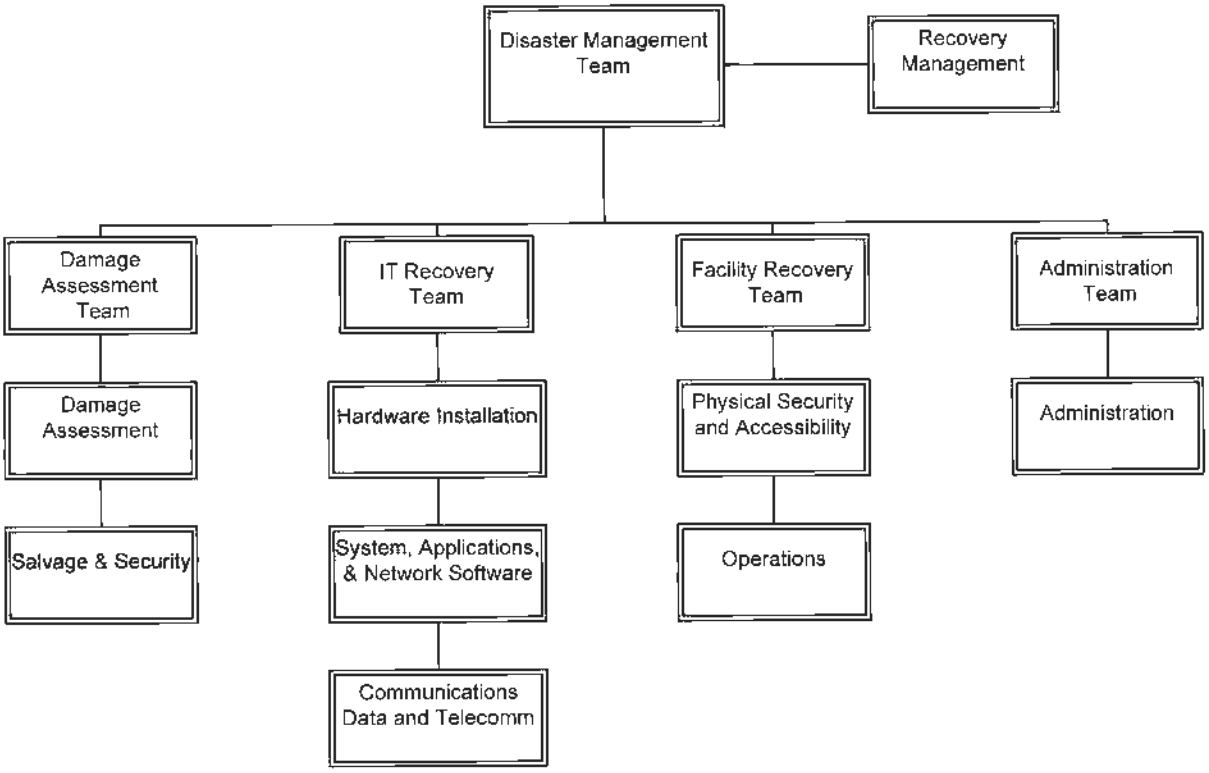
A recovery from a disaster is best conducted by teams of personnel that are formed to perform specific functions. The number and types of teams are dictated by the size and type of computer processing capabilities and the type of facility the DRP is being developed to recover.

The organization of the staff to recover the system is designed for the worst case situation. The worst case, requiring a move to the alternate site, must be executed by a coordinated team to minimize the operational impacts.

The Disaster Recovery Team Organization is set up to accomplish:

- Expeditious and efficient recovery of operations;
- Intermediate and minor impact/expenditure decisions within the Information Technology personnel during the recovery process;
- Major impact/expenditure decisions at the management level; and
- Streamline reporting of recovery progress from recovery teams upward to senior management and end-users.

5.1 Disaster Recovery Team Organization Chart



5.2 Disaster Recovery Team

Senior management will assign the members of the Disaster Recovery Team. They shall be reviewed at least once every twelve (12) months.

5.3 Disaster Recovery Team Responsibilities

5.3.1 Disaster Recovery Manager

The Disaster Recovery Manager is responsible for managing the recovery effort ensuring restoration occurs within planned critical time frames and assists in resolving problems requiring management action. All recovery teams report directly to the Disaster Recovery Manager. Specifically, the Disaster Recovery Manager is charged with:

5.3.2 Assessment Team

Responsible for the damage assessment of the facilities as quickly as possible following a disaster and reports the level of damage to the Disaster Management Team. The team secures the facilities to prevent unauthorized entry and provides personnel identification and access limitations to the facilities and acts as liaison with emergency personnel.

Specifically, the Damage Assessment Team is responsible for:

5.3.3 IT Recovery Team

The IT Recovery Team is responsible for the installation and configuration of all systems, including hardware and software.

The team is also responsible for the damage assessment of the data center facilities as quickly as possible following a disaster and reports the level of damage to the Disaster Recovery Manager.

5.3.3.1.1 Post-Disaster

- Retrieves communications configuration from off-site storage
- Plans, coordinates and installs communication and network equipment at alternate site
- Plans, coordinates and installs communication and network cabling at alternate site

5.3.4 Facility Recovery Team

The Facility Recovery team is responsible for providing the support to the Damage Assessment team for the general facilities of VisualVault offices and communicating with AWS representatives regarding the status of AWS data center locations.

5.3.5 Administration Team

The Disaster Recovery Administration team is responsible for providing secretarial, filing, procurement, travel and housing, off-site storage and other administrative matters not performed by other team members. Included is limited authority to provide funds for emergency expenditures other than for capital equipment and salaries.

6 Plan Administration

This Disaster Recovery Plan is a living document. Administration procedures are for the purpose of maintaining the Disaster Recovery Plan in a consistent state of readiness.

These procedures apply to the continued maintenance, testing and training requirements of the Disaster Recovery Plan.

The coordination of the Disaster Recovery Plan is the responsibility of the Disaster Recovery Manager.

The maintenance of this plan must take into consideration the impacts on information security. Guideless for the maintenance of this plan with respect to information security are located in the Document Management System (DMS) document ID ISO-0001. ISO-0001 must be reviewed during each plan review to ensure that the Disaster Recovery plan is compliance with GRM's information security requirements.

6.1 Disaster Recovery Manager

The function of the Disaster Recovery Manager is to assume a lead position in the ongoing maintenance of the plan and guide the Recovery Management Team in the event of a disaster. Maintenance of the Disaster Recovery Plan includes:

Distribution of the Disaster Recovery Plan

Maintenance of the Business Impact Analysis

Appointing the Disaster Recover Team

Training of the Disaster Recovery Team

Testing of the Disaster Recovery Plan

Evaluation of the Disaster Recovery Plan Tests

Review, change and update of the Disaster Recovery Plan

6.2 Distribution of the Disaster Recovery Plan

The Recovery Manager is responsible for the authorized distribution of the plan and the location of each plan copy. As this document is

confidential, the authorized distribution list must be approved by the VisualVault CTO.

The Plan reveals security information which should not be for general publication to non-participating employees or outsiders.

Customer requests to see this plan by a customer must be approved by the CTO and any confidential information including employee contact information, vendor contact information, and offsite storage details must be removed.

In addition to the Recovery Team members, one copy of the plan is maintained in a secure location at the Data Center Network location, and a secure location at the Corporate Network location. Additional copies of the Disaster Recovery Plan will be assigned to personnel on an as-required basis and as approved by the CTO. Each copy of this plan must be accompanied by a current network diagram, server configuration information, and backup tape decryption key.

The controlled copy of the Disaster Recovery Plan is located with the Corporate VisualVault database (Document ID ISO – 0015).

6.3 Training of the Disaster Recovery Team

It is the responsibility of the Disaster Recovery Manager to appoint and train the Recovery team members.

Records of team member training are stored within the VisualVault document management system (the plan has a training log within VisualVault).

6.4 Testing of the Disaster Recovery Plan

The Disaster Recovery Manager is responsible for testing of the Disaster Recovery Plan not less than once every year to ensure the viability of the plan.

The objectives of testing the Disaster Recovery Plan are as follows:

- To determine the effectiveness of the Plan procedures
- To determine the state of readiness and ability of designated Recovery Team personnel to perform their assigned recovery responsibilities
- To determine if the disaster recovery plan requires modifications or updates to ensure recovery within the Recovery Time Objective (TRO) and Recovery Point Objective (RPO) time frames

6.5 Maintenance of the Disaster Recovery Plan

The Disaster Recovery Manager is responsible for reviewing the Disaster Recovery Plan not less than once every year using the following checklist as a guide to determine if any updates must be made.

During each review, determine if the plan needs to be modified taking into consideration changes recorded in the ISO17779 information security system such as new risks identified since the last plan change.

Disaster Recovery Plan Annual Review Checklist

- ☑ Change in virtual machine configuration or network configuration
- ☑ Change in operating system and utility software programs
- ☑ Change in the design of production systems or files
- ☑ Addition of or deletion of a production system
- ☑ Change in the scheme of backing up data
- ☑ Changes in the voice or data network design
- ☑ Change in personnel assignments

- ☑ Change in off-site storage facilities, location or methods of data backup
- ☑ Review of Recovery Time Objectives (TRO) and Recovery Point Objectives (RPO).

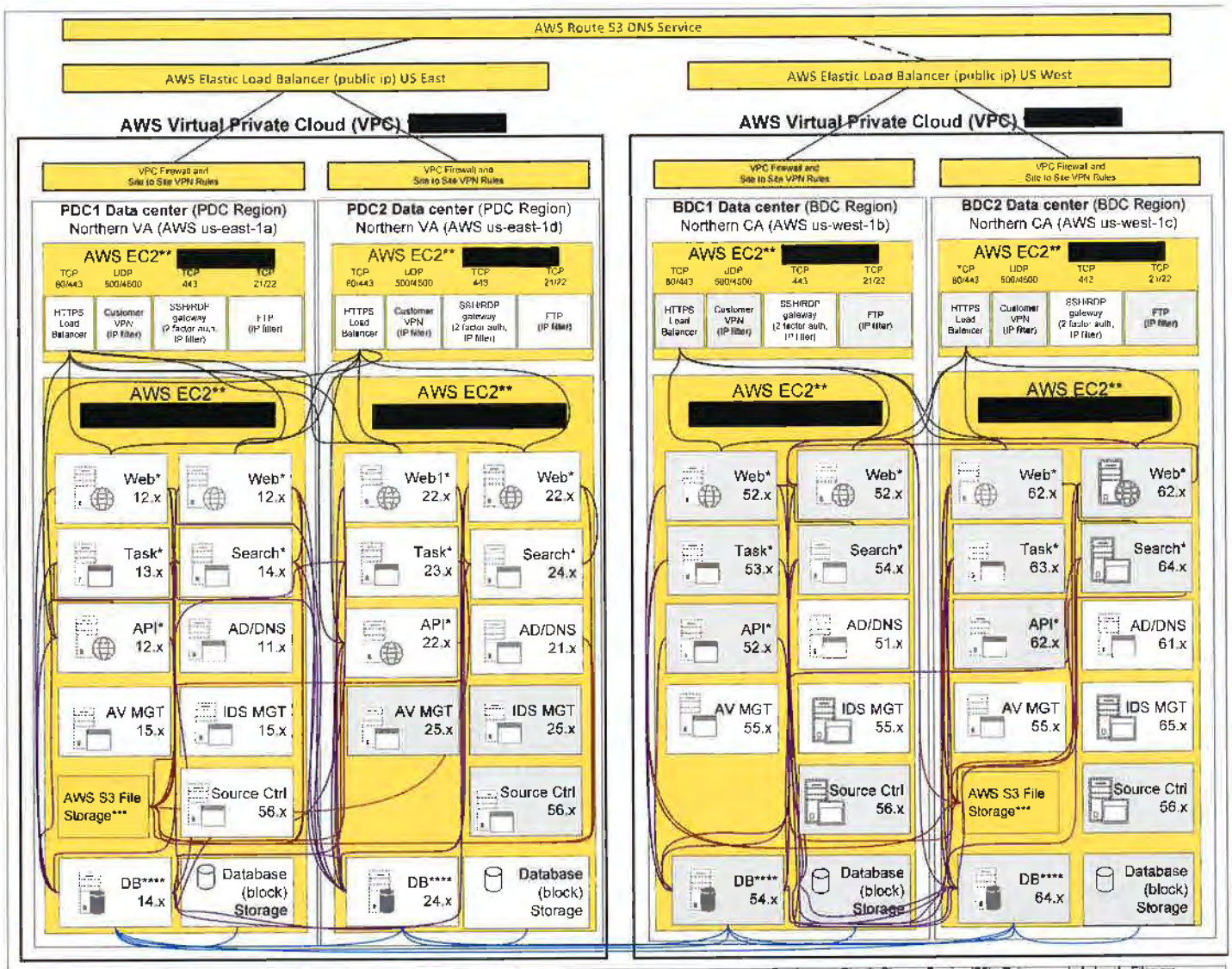


Diagram Name:	Physical Network Architecture		*Additional nodes added on demand	**AWS Elastic Compute Cloud single purpose network segments isolated by firewall rules	***Amazon Simple Storage Service (S3). Data encrypted at rest. Files are replicated between Northern VA and Northern CA AWS data center regions
Last Updated:	Dec 27 2016	Rev. 3	Confidential Document		****DB Asynchronous replication between data centers

Revision of this corporate standard is controlled by VisualVault Corporation's document management system (DMS). Copies can be obtained via the DMS. The master document (source file) is generated and maintained by Quality Assurance.

NOTE: Before using this document, make sure it is the latest revision. Access the DMS to verify the current revision.

Table of Contents

Revision History

Please refer to the DMS below for the complete revision history for this document:

STD-0001 Information Technology Security Standard

1 Purpose

VisualtVault (a GRM company) designs, develops, markets and supports Software as a Service (SaaS), which requires the storing and maintaining of customer data. VisualVault must maintain highly effective information technology (IT) security to meet customer requirements and regulatory requirements.

This standard establishes the processes and activities required for effective security management.

2 Scope

This standard addresses IT security processes and activities applicable to VisualVault, its clients and managed third parties.

VisualVault infrastructure utilizes two Amazon Web Services (AWS) primary data centers (PDC1 and PDC2) and two AWS backup data centers (BDC1 and BDC2). PDC1 and PDC2 are separate Availability Zones (data centers) located in Amazon's Northern Virginia Region; BDC1 and BDC2 are separate Availability Zones located in Amazon's Northern California Region.

All data center hardware and facilities are owned and operated by AWS.

AWS is responsible for the security of "Cloud" infrastructure including the following services used by VisualVault:

AWS Infrastructure	How used by VisualVault
Elastic Computer Cloud (EC2)	virtual servers, networking equipment
Elastic Block Store (EBS)	hard drives attached to EC2 compute resources, used by VisualVault to store database files, database log files, event logs, operating system files
Simple Storage Service (S3)	Object storage service used by VisualVault to securely store customer files, local and geographic replication, and storage of backup files
AWS Availability Zones (AZ)	AZs are Amazon data centers located within the same geographic region

VisualVault is responsible for the security of customer content and use of applications that make use of AWS infrastructure.

3 References

- Asset Listing Form (DMS IS – AL – 0019)
- VisualVault Encryption and Key Management document
- Disaster Recovery and Business Continuity Plan (VisualVault DR - BCP)
- Change Control Form (DMS SOP - 0003)

- Access Control Policy (DMS ISO - 0026)
- HIPAA and Patient Health Information Standard (DMS ISO - 0050)
- ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management (DMS ISO/IEC 27002:2005)
- IT Support Ticket (DMS IT-Support-00229)
- PCI Data Security Standard v2.0 (DMS PCI DSS v2.0)
- Data Retention Backup and Restore (DMS SOP-0009)
- VisualVault Information Security Risk Assessment Form (DMS IS - RA - 00007)

4 Abbreviations, Acronyms and Definitions

Term/Acronym/Abbreviation	Definition
Asset	Anything that has value to the organization and that must be controlled to safeguard corporate security
CEO	Chief Executive Officer
CFO	Chief Financial Officer
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature **NOTE:** Control is also used as a synonym for safeguard or countermeasure.
CSP	Cryptographic Service Provider
CTO	Chief Technology Officer
DHCP	Dynamic Host Configuration Protocol
DMS	Document Management System
Guideline	A description that clarifies what should be done and how to achieve the objectives set out in policies
HR	Human Resources
IEC	International Electro technical Commission
Information Processing Facilities	Any information processing system, service or infrastructure, or the physical locations housing them
Information Security	Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved
Information Security Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

Term/Acronym/Abbreviation	Definition
Information Security Incident	Indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
IP	Intellectual Property
IP Address	Internet Protocol address
ISO	International Organization for Standardization
IT	Information Technology
Local Environment	An environment in use and accessible by a single user
OSHA	United States Occupational Safety & Health Administration
Policy	Overall intention and direction as formally expressed by management
Risk	Combination of the probability of an event and its consequence
Risk Analysis	Systematic use of information to identify sources and to estimate the risk
Risk Assessment	Coordinated activities to direct and control an organization with regard to risk
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk Management	Process of selection and implementation of measures to modify risk
SaaS	Software as a Service
Disaster	Any interruption to operations that prompts a decision to execute a disaster recovery plan option.
Recovery Time Objective (RTO)	The target period of time by which a business service must be restored after a disaster or service disruption.
Recovery Point Objective (RPO)	The maximum acceptable period of data loss caused by a disaster or service disruption.
Cloud Computing	The on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the Internet.
Amazon Web Services (AWS)	Secure cloud computing platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow.

information should be given directly to the top HR manager. If the action may be against the top HR manager, the information should be given to the CEO. Refer to the company policies and procedures handbook and seek counsel from HR and/or the CEO regarding evidence leading to termination.

6.11 Business Continuity Management

6.11.1 Information Security Aspects of Business Continuity Management

6.11.1.1 Including Information Security in the Business Continuity Management Process

VisualVault maintains a comprehensive Disaster Recovery and Business Continuity Plan (DMS ISO - 0015).

ISO - 0015 has provisions for the secure transfer and storage of data during normal business operations and in the event of disaster.

6.11.1.2 Business Continuity and Risk Assessment

Business continuity risk assessment is managed in accordance with section 6.1 of this document.

6.11.1.3 Developing and Implementing Continuity Plans Including Information Security

Information security is a critical part of disaster recovery and business continuity planning. Changes to the Disaster Recovery and Business Continuity Plan must consider any impact on information security.

6.11.1.4 Business Continuity Planning Framework

The framework for disaster recovery and business continuity planning at VisualVault is as follows:

1. Maintain a comprehensive disaster recovery and business continuity plan.
2. Review the plan no less frequently than once per year.
    a. Determine the effectiveness of the plan and the readiness of the organization.
    b. Review the risk assessment history and consider the impact of identified risks on the plan.
3. The Disaster Recovery and Business Continuity Plan must consider information security requirements in the event of disaster including control over which recovery teams and company employees are allowed to communicate information or transfer data.

6.11.1.5 Testing, Maintaining and Reassessing Business Continuity Plans

Section 6 of the Disaster Recovery and Business Continuity Plan covers the administration of the plan. Specifically, the following items below must be included as part of the business continuity plan.

1. Training of the recovery team, which is appointed and trained by the disaster recovery manager
2. Testing of the recovery plan, which is the responsibility of the disaster recovery manager, including:
    a. Determining the effectiveness of the plan's procedures
    b. Determining the state of readiness

6.12 Compliance

6.12.1 Compliance with Legal Requirements

6.12.1.1 Identification of Applicable Legislation

VisualVault is committed to complying with all legal and contractual obligations. In addition, VisualVault will seek to comply with industry best practices and customers' regulatory requirements.

6.12.1.2 Intellectual Property Rights

VisualVault is committed to respecting intellectual property rights and to complying with all relevant legislation. To that end, VisualVault is committed to the following:

1. Acquiring software only through known and reputable sources to ensure that copyrights are not violated
2. Maintaining awareness of policies to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them
3. Maintaining proof and evidence of ownership of licenses, master disks and manuals
4. Implementing controls to ensure that any maximum number of users permitted is not exceeded
5. Using appropriate audit tools
6. Complying with terms and conditions for software and information obtained from public networks
7. Not duplicating, converting to another format or extracting from commercial recordings other than permitted by copyright law
8. Not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law

6.12.1.3 Protection of Organizational Records

VisualVault protects its records from loss, destruction and falsification.

6.12.1.4 Data Protection and Privacy of Personal Information

VisualVault strives to protect the privacy of personal information and the management of VisualVault has committed to being a leader in protecting and ensuring secure and confidential management of HIPAA compliant software systems, databases and associated hardware protections, as well as ensuring absolute confidentiality of any patient health information. VisualVault maintains a HIPAA and Patient Health Information Standard (DMS ISO - 0050).

6.12.1.5 Prevention of Misuse of Information Processing Facilities

VisualVault's Information Security Policy (section 6.2 of this document) outlines the controls required to prevent the misuse on its information processing facilities.

6.12.1.6 Regulation of Cryptographic Controls

VisualVault's Data Encryption SOP addresses cryptographic controls and their compliance with applicable law.

6.12.2 Compliance with Security Policies and Standards, and Technical Compliance

6.12.2.1 Compliance with Security Policies and Standards

Managers have the responsibility to ensure that all security procedures within their area of responsibility are carried out correctly and that all employees are trained adequately on all policies and procedures. When non-compliance is found in the manager's area they should:

- Evaluate and determine the reasons for non-compliance
- Evaluate the need for actions to ensure that the non-compliance does not happen again
- Implement corrective action
- Follow up on corrective action to ensure it is effective

When compliance issues are encountered during audits, a corrective action report should be filed and tracked.

6.12.2.2 Technical Compliance Checking

Technical compliance can be checked either manually or automatically depending on the system and the items that are being checked.

6.12.3 Information System Audit Considerations

6.12.3.1 Information System Audit Controls

When conducting audits of VisualVault information systems the following guidelines should be followed:

- All systems should meet the standards set forth in the company's policies and procedures.
- When a conflict is noted between two different policies, the policy that is most cost effective and minimizes the risk for VisualVault and its customers should be followed.
- The scope of an audit should be determined prior to each audit.
- The person carrying out the audit should be independent of the process being audited in order to give a fair assessment of compliance.
- All items checked in the audit should be documented along with their compliance results.
- Audit results should be provided to VisualVault management.

6.12.3.2 Protection of Information Systems Audit Tools

Access to audit tools and preliminary audit results should be controlled in order to prevent tampering with and skewing audit results. Results should be stored and protected as soon as possible after the information is captured.

Author(s): Les Fisher

Approver(s): Please refer to the DMS document below for a list of approvers.
SOP-0006 Software Development Life Cycle

Revision of this standard operating procedure (SOP) is controlled by VisualVault's document management system (DMS). Copies can be obtained via the DMS. The master document (source file) is generated and maintained by Quality Assurance.

NOTE: Before using this document, make sure it is the latest revision. Access the DMS to verify the current revision.

Table of Contents

Revision History

Please refer to the DMS document below for complete revision history.

SOP-0006 Software Development Life Cycle

1 Purpose

This document defines the concepts and requirements for the life cycle for software development at VisualVault. Following the software development life cycle (SDLC) model is critical for achieving compliance with industry standards and is a prerequisite for computerized systems validation. This standard operating procedure (SOP) describes the life cycle model, and the processes, activities and tasks associated with the various stages of the model.

2 Scope

This SOP is applicable to all software applications and database systems developed at VisualVault.

This SOP describes the activities that should be carried out during the development of these software applications and database systems, and covers hardware, software and network components.

This SOP applies to the development of new software applications and database systems, and to changes made to existing software applications and database systems.

3 References

- Change Control SOP (DMS SOP-0003)
- Coding Standards SOP
- Configuration Management SOP (DMS SOP-0008)
- IT Security Standard (DMS STD-0001)
- PCI Data Security Standard v2.0 (DMS PCI DSS v2.0)
- System Risk Assessment SOP
- VisualVault Quality Manual (DMS QM)

4 Abbreviations, Acronyms and Definitions

Term/Acronym/Abbreviation	Definition
CMT	VisualVault's Code Management Tool, which is Team Foundation Server
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature **NOTE:** Control is also used as a synonym for safeguard or countermeasure.
CTO	Chief Technology Officer
DMS	VisualVault's Document Management System
IQ	Installation Qualification
OQ	Operational Qualification
PQ	Performance Qualification (also called UAT or User Acceptance Test)
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk

Term/Acronym/Abbreviation	Definition
SDLC	Software Development Life Cycle
SOP	Standard Operating Procedure
SRS	Software Requirements Specification
VisualVault	Used interchangeably with VisualVault in this document

5 Responsibilities

VisualVault management is responsible for the implementation of this SOP and for ensuring that all employees and contractors involved in the software development process are adequately trained in this procedure.

All VisualVault employees and contractors involved in the software development process are responsible for adherence to this SOP.

The VisualVault quality assurance function is responsible for monitoring compliance with this SOP.

6 Procedure

6.1 Overview

The life cycle is the period of time that starts when a system is conceived and ends when the system is no longer available for use.

The life cycle model requires the system owner to be in control of the system at all times and be able to provide appropriate supporting documentation.

Application of the model enables the presentation of the system's history and planned future in a consistent manner.

Qualification and validation principles and activities for systems covered by government regulations are supported by the life cycle model.

Not every system goes through every stage of the life cycle model and some systems may require additional stages. This is permissible but the system documentation must detail the reasons.

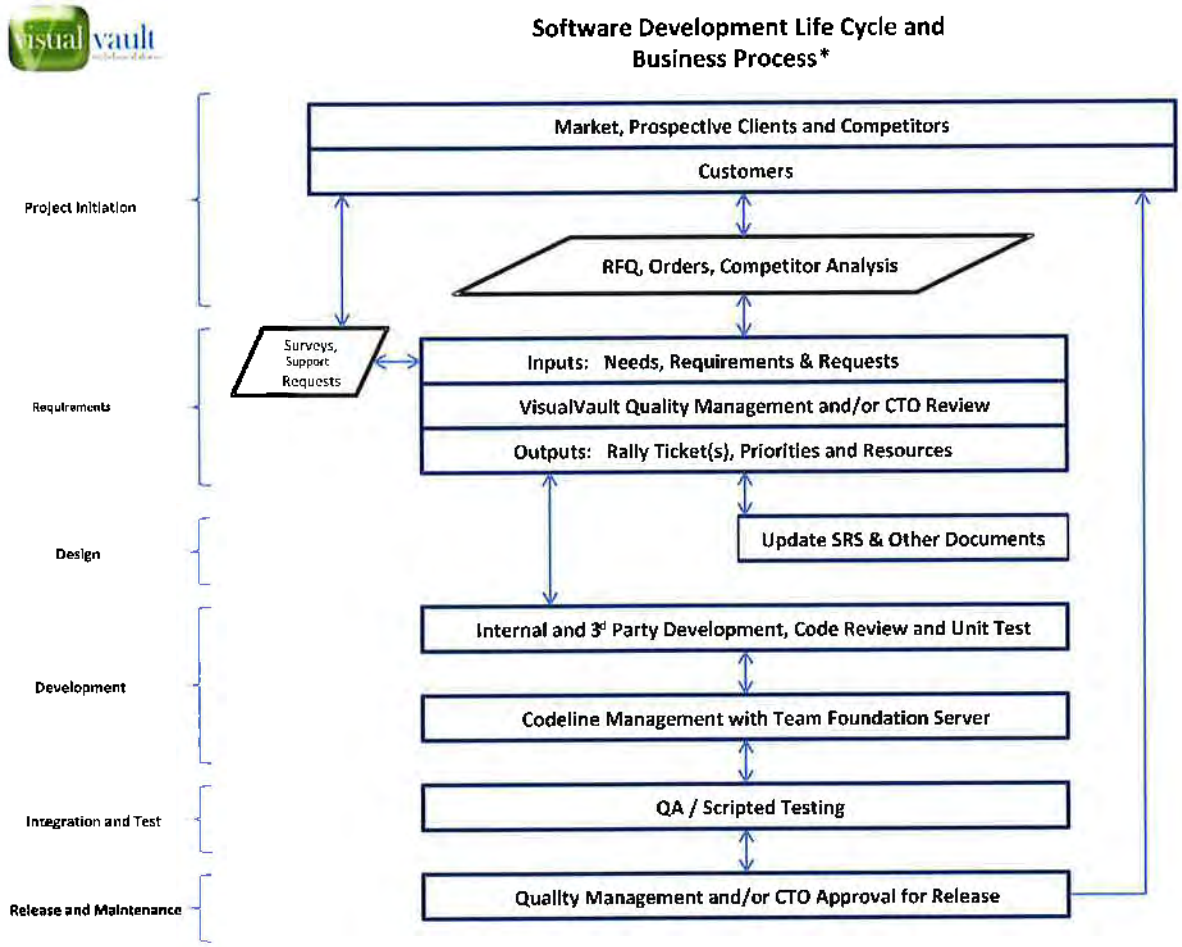
The various stages of the life cycle model may be addressed in a linear (strictly consecutive) or in an iterative manner. System documentation should describe the approach and provide an appropriate rationale.

Risk management activities should be integrated into the life cycle model where appropriate.

The SDLC model has the following six phases:

1. Project Initiation
2. Requirements
3. Design
4. Development
5. Integration and Test
6. Release and Maintenance

The following diagram illustrates the SDLC within the context of VisualVault's business process:



* The SDLC is generally an iterative process with phases being addressed in an order appropriate for the system being developed

6.1.1 Project Management

All or part of a system's life cycle activities may be managed through project management methodologies. Application of these well-established methodologies permits following predefined processes with clearly established milestones and associated deliverables. It is recommended to apply good project management practices.

6.1.2 Risk Management

A risk based approach to testing may be taken by evaluating the risk of a system's functional requirements and tailoring the level of testing for each requirement to its corresponding level of risk.

6.1.3 Configuration Management

Configuration management is ongoing during the SDLC to ensure that only authorized changes are made to software designs.

Source code shall be version controlled with VisualVault's code management tool (CMT) in a manner consistent with the Configuration Management SOP.

6.1.4 Change Control

Changes to a system following its deployment to the production environment should be initiated in a manner consistent with the Change Control SOP.

6.2 Project Initiation Phase

Software development projects are initiated in response to customer requests and via proactive initiatives by VisualVault. A software development plan should be created to identify the development objectives. A separate project plan with a timeline and key milestones may also be created.

6.3 Requirements Phase

During the Requirements phase of the SDLC, the customer's business and functional requirements are identified. The role of the software is defined. All requirements, including such things as security, audit trail, user interface, data, environmental, performance, implementation and hardware requirements should be documented.

Once a system's requirements have been identified, each requirement may be evaluated for its level of business risk. A risk assessment may be documented for each requirement based on the metrics described in the System Risk Assessment SOP. The testing strategy for each requirement may then be tailored to its risk level in a manner consistent with the methodology described in the System Risk Assessment SOP. Any risk-based testing strategy should be detailed in the test plan.

6.4 Design Phase

During the Design phase, analyses are conducted to identify the most efficient way to logically implement the software requirements. Each requirement should be addressed by at least one design element. The considerations used to develop the design are documented in the Software Requirements Specification (SRS). The SRS serves as the basis for development, design verification, test plans and test cases.

6.5 Development Phase

6.5.1 Coding

Software source code is written based on the SRS, which has been developed to meet the system requirements. The format and content of the source code should be consistent with the software coding standards described in the Coding Standards SOP.

6.5.2 Code Review and Unit Testing

The source code for each module shall be reviewed to verify its compliance with VisualVault coding standards and the SRS. This code review should be completed prior to unit testing.

Unit testing shall be conducted in the development environment to exercise and verify the program logic, including such items as the control structures, the boundary conditions, computations, comparisons and control flow. Unit testing should be completed and approved prior to integration testing. When necessary, appropriate corrections will be made to the source code and supporting documentation during and/or following unit testing.

6.6 Integration and Test Phase

During this phase, the software is further tested in the development environment and then moved to a dedicated test environment that is substantially the same as the production environment. All testing in the test environment is executed via test scripts, which detail testing tools (if any), preconditions, acceptance criteria and expected results.

6.6.1 Integration Testing

When unit testing has been completed and approved, integration testing is performed in the development environment to ensure that the individual modules work together, all functionality exists and the software is trustworthy. Integration testing shall be executed prior to installation qualification

(IQ) testing. When necessary, appropriate corrections will be made to the source code and supporting documentation during and/or following integration testing.

6.6.2 Test Plan

When integration testing has been completed, a test plan shall be prepared to identify the scope of testing to be performed as well as the individual tests that will be executed. The test plan shall be approved by the Chief Technology Officer (CTO) or a designee.

6.6.3 Installation Qualification

IQ is performed for the transition from the development environment to the test environment. IQ is designed to ensure that hardware and software are installed according to the installation design of the developer. It is documented proof that the installation was done according to the developer's specifications.

Defects, anomalies, inconsistencies and errors found during IQ testing are entered into an electronic error tracking database, documented and traced back to the source document. When corrective actions are required, appropriate regression testing should be performed.

6.6.4 Operational Qualification and Performance Qualification

When IQ testing has been completed, operational qualification (OQ) and performance qualification (PQ) testing are performed. OQ and PQ testing should ensure that the system operates as defined in the SRS and should challenge the system to fail to ensure the system does not perform in unintended ways. OQ typically tests all operational requirements while PQ (also called user acceptance testing) typically tests daily business usage requirements. OQ and PQ may be done separately or as one test set as long as all testable requirements are covered.

Test specifications should include clear, detailed instructions and acceptance criteria, and provide a means for recording observed results, the tester, and the date the test was executed. When necessary, appropriate corrections will be made to the source code and supporting documentation during and/or following OQ and PQ testing.

The OQ and PQ tests are preferably performed in the test environment. The tests of functions and facilities can be tested with the aid of simulation hardware and/or software. Automated testing tools may also be used if desired.

Testing of the software is done against the SRS. The functional risk assessment, if created, serves as a guide to determine the depth and extent of testing, including stress testing such as boundary testing and challenge testing.

To enhance software safety and reliability, multiple analysis and verification techniques should be used to maximize error detection.

Defects, anomalies, inconsistencies and errors found during OQ and PQ testing are entered into an electronic error tracking database, documented and traced back to the source document.
When corrective actions are required, appropriate regression testing should be performed.

6.6.5 Test Summary Report

The results of testing activities shall be documented and maintained for review. A test summary report shall be prepared following successful OQ and PQ testing. The report should provide a summary of all testing activities. Any unresolved test failures shall be described and appropriate workarounds documented. A recommendation for whether to release the system to the production environment shall also be included.

6.7 Release and Maintenance Phase

6.7.1 Release to Production

Release of the system for use in production must be authorized. The test summary report shall be approved in the DMS, at a minimum, by the CTO or a designee prior to releasing the system in the live environment.

Releases must be coordinated with the users and must include suitable training. On release, the system should be verified as operational in the live environment via a non-destructive OQ.

6.7.2 Maintenance

All reported problems and maintenance activities for the system shall be recorded and tracked to remediation in a defect tracking system.

Implementation Guidance

Project Management and Testing Methodologies

Contents

1 Project Management Methodology

VisualVault's Project Management Methodology is based upon Agile principles and incorporates the following project management.

1.1 Pre-Planning Session

This session will be held to organize the implementation plan into Citizen's Enterprise Rhythm cadences, establish the roles and responsibilities across the implementation team, and ensure both Citizens and Visual Vault role & expected responsibilities are met. The pre-planning session will also identify the features/functions that will need to have current state business processes and procedures reviewed during Discovery.

1.2 Discovery

During this phase of the project, we meet with subject matter experts, project stakeholders and customer leadership to understand the needs of the organization, the business processes, roles of individuals involved in the process, security and reporting needs. We seek to identify issues and bottle necks in the current process. We seek to suggest solutions to resolve current issues.

1.2.1 Requirements Specification Document

The Discovery phase deliverable is a detailed requirements specifications document that outlines how the system will be configured to meet the needs and scope of the project.

The requirements specifications document will include:

- Requirements which elaborate on the scope of work including business process flows and UI mockups,
- Implementation strategy,
- Conceptual sprint roadmap,
- Resource staffing plan,
- Defined current state of the business processes and procedures that require changes for future state,
- Definition of reports and dashboards required,
- Data conversion requirements and data conversion conceptual sprint plan,
- Integration downstream and upstream blueprints

1.3 Sprints and Sprint Planning

Sprints are a pre-defined period in which a specific unit of testable work is completed.

Each Sprint starts with Sprint planning which includes further elaboration of the feature definitions documented during Discovery. The elaboration process may provide details not captured during Discovery.

Sprint planning is completed by the project manager and implementation team members. However, the implementation team members have final say in the scope of each Sprint.

Sprint planning focuses on delivering a testable set of requirements as defined in the requirement specifications document. This approach allows the customer to begin testing early and continue testing throughout the project duration.

Each Sprint includes:

- Elaboration of a feature defined in the requirement specifications document,
- Configuration or development effort,
- Unit and feature testing,
- Demonstration,
- Sprint Level User Acceptance Testing (UAT) by the customer

1.4 Production Implementation

Feature components "exiting" from development Sprints and defined as 'done' are released into a "sandbox" environment. The Sandbox environment is a production like environment that will accumulate all 'done' feature components (including 'done' integrations). The Sandbox environment is considered a 'model office' environment that will be used 'on-going' by the business users to confirm business process and procedure changes, planning for training and communications and be a 'ready' product for production deployment.

The Production system is setup with configurations from the Sandbox environment. Once Solution/System User Acceptance Test is completed and the system is approved for production deployment, the VisualVault implementation team conducts final production migration.

1.5 Project Closeout and Support

Once Project Acceptance has taken place the we start a 30-45-day transition period from our Professional Services team to our Support team. This transition means that issues will be logged in our Support system but will be managed by the team that delivered the solution to the customer.

2 Testing Methodology

The VisualVault system implementation testing methodology goal:

"Constantly deliver software that meets or exceeds the customer's requirements by means of providing fast feedback and focusing on defect prevention rather than defect detection.

2.1 Unit Testing

Testing is the responsibility of everyone involved in the project. Developers and system integrators are responsible for unit testing (either automated or manual) each Sprint's deliverables prior to the Sprint Level customer UAT.

2.2 Sprint Level User Acceptance Testing (UAT)

Each Sprint must include customer User Acceptance Testing to be considered done. Sprint planning should update the project test plan with UAT test cases related to the Sprint.

2.3 System Level User Acceptance Testing (UAT)

Each Sprint includes Sprint Level User Acceptance Testing (UAT) performed by the customer. Sprint Level UAT is a requirement for considering a Sprint to be 'done'.

When all Sprints are completed, or when all Sprints related to a Program Increment are completed, System Level User Acceptance Tests can be performed.

System-level User Acceptance Tests (UAT) are business-facing tests which validate behavior of the whole system as described in the requirements specification document.

2.4 Performance Testing

As described and agreed upon in the requirements definitions document and/or statement of work. Reasonable load should be applied to the Sandbox environment prior to final UAT in order to discover bottlenecks that may result from migrated data, inefficient business process automation scripts, etc.

2.5 Data Migration Conversion Testing

As described and agreed upon in the requirements definitions document.

3 Post Production Support SLA

3.1.1 SERVICE LEVEL AGREEMENT FOR SUPPORT

1. **On Call Support.**
   1.1. The Principal Period of Support ("PPS") is a ten (10) hour contiguous daily time between the hours of 8:00 AM and 5:00 PM, Eastern US local time, Monday through Friday, excluding VisualVault's (VVs) published holidays or holidays as observed locally by VV. All Support subsequently added will have the same PPS.
   1.2. Twenty-four (24) hour premium support services are available to Citizens for $1,150.00/month. Extended Hours Entitlement extends the Client's ability to place problem calls to VV's Technical Services Group ("TSG") during the extended hours of coverage period and receive the same priority remote response for critical issues as during the PPS.

2. **Severity Levels.**

Based on communications between Subscriber and VV, the parties shall determine, in accordance with the following table, the "Severity Level" of each issue.

Severity Level	Definition
1	An issue that causes the Software to crash or be unavailable for use and which has no acceptable work-around. OR "Critical" rated security vulnerability as defined by the Common Vulnerability Scoring System (CVSS) qualitative severity rating scale.
2	An issue that affects multiple users of the Software and prevents effective use of an essential feature or essential features of the Software, but which does not cause the Software to be unavailable for use in whole. OR "High" rated security vulnerability as defined by the Common Vulnerability Scoring System (CVSS) qualitative severity rating scale.
3	An issue that affects productivity or ease of use of the Software and for which there is typically a work around. OR "Medium" rated security vulnerability as defined by the Common Vulnerability Scoring System (CVSS) qualitative severity rating scale.
4	An issue that does not materially affect Subscriber's (or any Subscriber Customer's) ability to use the Software (e.g., user interface inconveniences) OR a documented non-compliance issue.

Based on the "Severity Level" of the issue, each of VV and Subscriber shall take the following actions:

Severity Level	VV Responsibilities	Client Responsibilities
1	Acknowledge and begin addressing immediately. VV's Client support and production support teams will work continuously until fixed, 24x7 if not resolved by the close of the business day. Such 24x7 effort to commence first business day after determination of severity. Target resolution time is four (4) hours.	Call at time of discovering issue (email not acceptable for Severity 1). Be available to answer questions, provide information, and receive and install code fix immediately, 24x7 if not resolved by the close of the business day.
2	Acknowledge and begin addressing promptly. VV's Client support and production support teams will work continuously within normal business hours until resolved. Target resolution time is 24 hours.	Be available to answer questions, provide information within four (4) hours of request. Install/test fix providing feedback.
3	Acknowledge within one business day. Issue will be scheduled to be addressed, based on the priority set by Client and VV. Target resolution time is seven (7) days.	Provide information and answer questions within one (1) business day.

4 Project Deliverables Example

Summary table of project deliverables grouped by type. The table below comes from the PERT Excel Template. Its simpler to fill in this table in Excel and then copy/paste the table.

Deliverable	Description
Project Planning	
Project Plan Creation	Project plan creation and project setup
Business Analysis	
Discovery	
Specifications Document	Documents all required forms, business process flows, reports, customer business logic and data validation, external system integration requirements
Build Test Plan	Test plan will be created upon completion of requirements specification and updated as necessary during each sprint planning session
Business Process 1	
New Agency Onboarding	
New Agent Onboarding including Appointment Process	
Invoicing (fees, refunds, credits)	
Business Process 2	
Agent Licensing Processes	

Credit Check	
Data Migration	
Data Dictionary	Build data dictionary
Analysis	Perform analysis and document data migration tasks
Test Migrations	Perform test data migrations
Production Migration	Final production data migration
Testing	
Sprint Level UAT	**UAT performed on conclusion of each Sprint**
System-Level UAT & defect resolution	System Testing upon completion of each Program Increment
Integration Testing	Integration environment testing upon each sprint completion
Training Materials	
Customer Training Manual	Create training manual documenting all business processes
Training	
Train the Trainer (3 @ 2 Day Training)	On-site classroom training
Admin Training (5 Days)	On-site classroom training
Agency management staff training (3 @ 2 Day Training)	On-site classroom training
Post implementation webinars (3)	Online
Support Training (3 Days)	On-site classroom training

Revision of this standard operating procedure (SOP) is controlled by VisualVault's document management system (DMS). Copies can be obtained via the DMS. The master document (source file) is generated and maintained by Quality Assurance.

NOTE: Before using this document, make sure it is the latest revision. Access the DMS to verify the current revision.

Table of Contents

Revision History

Please refer to the DMS document below for complete revision history.

SOP-0003 Change Control

1 Purpose

The purpose of this standard operating procedure (SOP) is to define the procedures for change control for all computerized information systems at VisualVault.

2 Scope

This SOP is applicable to all VisualVault computer hardware, network infrastructure, software (including custom and commercial off-the shelf systems) and data repositories supporting production-ONLY systems.

3 References

- Change Control Google Sheet
- IT Security Standard
- Software Development Life Cycle

4 Abbreviations, Acronyms and Definitions

Term/Acronym/Abbreviation	Definition
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature **NOTE:** Control is also used as a synonym for safeguard or countermeasure.
CTO	Chief Technology Officer
DMS	VisualVault's Document Management System
SOP	Standard Operating Procedure
VV	Used interchangeably with VisualVault in this document

5 Responsibilities

VisualVault management is responsible for the implementation of this SOP and for ensuring that all employees and contractors involved in the change control process are adequately trained in this procedure.

All VisualVault employees and contractors involved in the change control process are responsible for adherence to this SOP.

The VisualVault quality assurance function is responsible for monitoring compliance with this SOP.

6 Change Management Procedure

6.1 Initiate a Change Request

6.1.1 Software Development Change Control

All software development change control is managed using Microsoft Team Foundation Server (TFS) and Team City build automation server. We have established workflows within TFS to ensure each development task or defect is routed through through a QA workflow.

6.1.2 Change Control Form (non-software development)

All requests for change must be documented and shall be initiated using the change control form located at https://na3.visualvault.com/app/VisualVault/Main The change control form includes the following required fields:

- Date
- Type (Planned or Emergency). Emergency is reserved for security threats or downtime situation.
- Location (i.e. Development, Sandbox, or Production Environment). If Production environment see section 6.7, Implementation of Changes in Production Environments.
- Impact on Production
- Description of Change – a clear description of the change with justification
- Employee
- Comments

6.2 Obtain Approval to Proceed

Any change request should be assessed prior to approval by a defined set of people with the knowledge and experience to ensure that the impact of the change has been fully defined and understood.

The Change Log entry must be approved by the CTO, Senior Network Engineer, or Product Manager.

6.3 Develop and Test

Where appropriate, an implementation plan or project plan shall be generated to show the number of activities required to implement the change. This plan should include activities such as code change, environment change, testing, back out/recovery and documentation.

Changes shall be made in accordance with the change request, implementation plan or project plan. All work shall be performed, reviewed and tested prior to being released in the live environment in a manner consistent with the level and formality as specified in current standards and SOPs (e.g. network and hardware qualified in accordance with the Infrastructure Qualification SOP and software tested in accordance with the Software Development Life Cycle SOP).

6.4 Complete Documentation

All documents associated with the change shall be updated as required. This shall include, at a minimum, the completed change request, and any plans and testing documentation.

6.5 Obtain Approval to Release (software development changes)

Release of software must be authorized by the CTO or Product Manager. Software release changes and QA acceptance are recorded in the version control repository (TFS).

6.6 Software Release

Upon release, software builds must be validated as operational in a sandbox environment prior to scheduling an update to production environments.

6.6.1 Release Schedule

6.6.1.1 All customers

Patches are typically released monthly and require 7 days advance notice.

6.6.1.2 Multi-tenant customers

Minor version upgrades are typically released quarterly and require minimum of two weeks advance notice.

Major version upgrades are typically released annually and require minimum one-month advance notice.

6.6.1.3 Dedicated instance customers who have purchased a Sandbox Environment

Minor version upgrades are typically released quarterly. Customer sandbox environment will be updated at the time of the release notification. Customer production environment will be updated upon customer approval (typically involves customer testing within the sandbox environment).

Major version upgrades are typically released annually. Customer sandbox environment will be updated at the time of the release notification. Customer production environment will be updated upon customer approval (typically involves customer testing within the sandbox environment).

6.7 Notification Process

Patches: Seven days advance notice unless deemed an emergency (security) patch

Minor version upgrade: Two weeks advance notice posted to https://status.visualvault.com

Major version upgrade: One-month advance notice posted to https://status.visualvault.com

Customers may subscribe to notifications at https://status.visualvault.com

7 Production Environment Notification Process

Production environment changes must first be approved in accordance with section 6 of this operating procedure.

Minimum advance notification of change must be posted or transmitted according to the tables below.

Notification type legend

Type	Description
System Status	**Posted to system status public web page**
Announcement	**Login page announcement text**
Customer Email	**Email to customer system status distribution list**
Internal Email	**Email to internal system status distribution list**

Notification type and minimum notice period

Type	Impact	Notification Type	Minimum Notice Period
Planned	**Downtime Likely**	System Status, Announcement, Customer Email, Internal Email	7 days
Planned	**Downtime Unlikely**	System Status, Announcement, Customer Email, Internal Email	7 days
Planned	**No Impact**	Internal Email	24 hours
Emergency	**Downtime Likely**	System Status, Announcement, Customer Email, Internal Email	none
Emergency	**Downtime Unlikely**	System Status, Announcement, Customer Email, Internal Email	none
Emergency	**No Impact**	Internal Email	none

Approver(s): Please refer to the DMS at the following link for a list of approvers.

Revision of this standard operating procedure (SOP) is controlled by VisualVault Corporation's document management system (DMS). Copies can be obtained via the DMS. The master document (source file) is generated and maintained by Quality Assurance.

NOTE: Before using this document, make sure it is the latest revision. Access the DMS to verify the current revision.

Table of Contents

1 Revision History

Please refer to the DMS for the complete revision history for this document.

2 Purpose

Backup and Restore Procedures

3 Scope

This document defines backup and restore procedures for the following data:

- Customer database files
- Database log files

- Customer files uploaded to a VisualVault instance
- Virtual machine image files (server images)

4 Abbreviations, Acronyms and Definitions

Disaster is any interruption to operations that prompts a decision to execute a disaster recovery plan option.

Recovery Time Objective (RTO) is the target period of time by which a business service must be restored after a disaster or service disruption.

Recovery Point Objective (RPO) is the maximum acceptable period of data loss caused by a disaster or service disruption.

Cloud Computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the Internet.

Amazon Web Services (AWS) is a secure cloud computing platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow.

Amazon Elastic Compute Cloud (EC2) is a set of AWS services that provide scalable computing capacity within the Amazon Web Services (AWS) cloud. EC2 allows customers to launch virtual servers (EC2 instances) as needed, configure security and networking, and manage storage.

AWS Virtual Private Cloud (VPC) is a virtual network logically isolated from other virtual networks in the AWS cloud. AWS resources, such as Amazon EC2 instances, are launched within a VPC. Each VPC has a configurable IP address range and can contain subnets, route tables, network gateways, and firewall rules.

AWS Regions and Availability Zones (AZs) Amazon EC2 is hosted in multiple locations world-wide. These locations are composed of regions and Availability Zones. Each *region* is a separate geographic area. Each region has multiple, isolated data center locations known as *Availability Zones*. Amazon EC2 provides the ability to place resources, such as instances, and data in multiple locations. Resources can be replicated across regions.

Amazon Simple Storage Service (S3) is a secure object storage service used to store and retrieve any amount of data. S3 is designed to deliver 99.999999999% durability, and scale past trillions of objects worldwide. S3 is used as a bulk repository for analytics, backup & recovery, disaster recovery, and primary storage for many cloud-native applications.

Primary and Backup Data Center Locations (PDC1, PDC2) (BDC1, BDC2) VisualVault infrastructure utilizes two primary data centers (PDC1 and PDC2) and two backup data centers (BDC1 and BDC2). PDC1 and PDC2 are separate Availability Zones (data centers) located in Amazon's Northern Virginia Region; BDC1 and BDC2 are separate Availability Zones located in Amazon's Northern California Region.

5 Responsibilities

Monitoring and configuration of backup and restore jobs is the responsibility of the VisualVault data center operations team.

6 Procedure

All customer data must remain encrypted at rest always following the encryption and key management policy.

VisualVault relies on a combination of commercial backup software and AWS services to backup customer data and uses geographic separation of data backups to minimize risk.

All customer data is encrypted at rest and replicated from a Primary Data Center to two other Data Center locations including at least one geographically separated Data Center location.

Off-site backup archives (export from AWS S3 storage service to encrypted hard drives) are performed by customer request only and additional fees apply.

Backup procedures are defined in the following table:

Type of Data	Interval	Software	Backup Procedure	Retention Period
SQL Database Files	**Nightly**	Idera SQL Safe	Nightly, Weekly, and Monthly scheduled full backup to disk. Idera SQL Safe backup software automatically detects new databases and creates a SQL data file backup schedule based upon a pre-defined template.	2 Weeks on disk
	Nightly	Cloudberry AWS Backup Professional	Copy SQL backup files to AWS S3 bucket	See data retention schedule
	Continuous	AWS S3 Policy	Once saved to AWS S3, database backup files are replicated to a geographically separated data center location.	See data retention schedule
SQL Log Files	**15 minutes**	Idera SQL Safe	Scheduled SQL log file backup to disk Idera SQL Safe backup software automatically detects new databases and creates a SQL log file backup schedule based upon a pre-defined template.	1 Week on disk
	15 minutes	Cloudberry AWS Backup Professional	Copy SQL log backup files to AWS S3 bucket	See data retention schedule
	Continuous	AWS S3 Policy	Once saved to AWS S3, log files are replicated to a geographically separated data center location.	See data retention schedule
Customer Files	**Continuous**	AWS S3 Policy	Continuous, asynchronous, data replication within AWS region and also to the backup data center geographic location.	See data retention schedule

7 Data Retention Schedule

Type of Data	Backup Interval	Retention period
SQL database files	**Daily**	2 Weeks or SLA requirement
	Weekly Database Backup	3 Months or SLA requirement
	Monthly Database Backup	1 Year or SLA requirement
	Yearly Database Backup	10 Years or SLA requirement
SQL log files	**15 minutes**	1 Week
Customer files	**Continuous**	Indefinite or as defined by customer within VisualVault.
Purged customer files	**Continuous**	1 Month or SLA requirement

As required by the disaster recovery plan, the backup procedures replicate backup media to the Backup Data Center using AWS S3 replication. The Backup Data Center is geographically separated from the Primary Data Center (see Network Diagram for data center locations).

8 Data Restore

All customer data must remain encrypted at rest always following the encryption and key management policy.

8.1 SQL Database Restore

If a restore needs to take place, the authorized staff will copy backup media (SQL data files and log files) from Amazon S3 to a volume attached to the Idera SQL Safe backup server(s).

Once the SQL backup media is accessible to the SQL Safe backup software, restore operations are initiated using the SQL Safe backup software user interface.

8.2 Customer File Restore

Customer files uploaded to VisualVault are stored in an S3 bucket with S3 versioning enabled. Files are continuously replicated by AWS within the same region and also backed up to an S3 bucket located in the Backup Data Center region.

The AWS S3 file versioning feature prevents files from being modified or deleted. Each change to a file results in a new "version" of the file being created and replicated to the Backup Data Center region. If a file is purged within VisualVault, the file is not immediately deleted from the S3 buckets.

Process for restoring customer files located in an S3 bucket:

- Identify the S3 bucket location where VisualVault expects to find the customer files.
    - Log into the VisualVault instance used by the customer and navigate to the Central Admin screen. This action requires VisualVault "configuration admin" privileges.
    - Navigate to the Customers/Customer Databases" menu location and search for the customer database
    - Open the database properties and navigate to the Content Stores tab. Locate the S3 content store and click to view its properties. The content store properties will display the S3 geographic region code and bucket name where VisualVault expects to find the customer's files.
    - Record the Customer unique identifier and Customer Database unique identifier which are visible in the Central Admin URL when looking at the content store properties screen.

- The S3 full path where VisualVault expects to find customer files is [Bucket Name]/[Customer Unique Id]/[Database Unique Id]/[File Revision Unique Id].[Extension]
- Use S3 API calls to copy the files to be restored from the source S3 bucket location to the target S3 bucket location where VisualVault expects to find the files. If files with matching S3 key names exist, S3 versioning will create a new version of the files.

Data at Rest Encryption and Key Management

Revised February 2016

Table of Contents

Introduction

Encryption and decryption require three primary components: (1) the data to be encrypted or decrypted; (2) the encryption method also known as the encryption algorithm; and (3) the encryption keys used in conjunction with the encryption algorithm.

Encryption Keys

An encryption key is information used to change the outcome of an encryption algorithm. Without the key, the algorithm would not produce secure cipher text. Once data has been encrypted, the encryption key is required to decrypt the cipher text.

Management of encryption keys and protecting the keys from unauthorized access is critical. Effective key management requires a Key Management Infrastructure (KMI).

Encryption algorithms

Symmetric encryption

Symmetric encryption is also known as "Two-Way" encryption or "Secret Key" encryption. A single encryption key is used to both encrypt and decrypt data. This type of encryption relies on block level encryption so it may be used to encrypt large amounts of data making it suitable for file encryption.

Symmetric encryption is ideal for file encryption but poses a problem for effective encryption key management. Changing a symmetric encryption key potentially requires decrypting and re-encrypting all files protected by that key.

A common algorithm for symmetric encryption is the Advanced Encryption Standard (AES).

Asymmetric encryption

Asymmetric encryption is also known as "one-way encryption" or "Public Key" encryption. Asymmetric encryption requires a public and private key pair along with a Public Key Infrastructure (PKI) which is used to generate and manage the keys.

A common algorithm for asymmetric encryption is RSA. Asymmetric encryption algorithms such as RSA are limited mathematically in how much data they can encrypt. Asymmetric encryption is performed on a small number of bytes and useful only for small amounts of data.

VisualVault Data at Rest Encryption

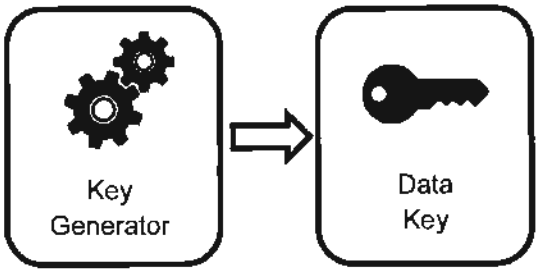
Summary

VisualVault uses a combination of symmetric and asymmetric encryption algorithms called "Envelope Encryption" along with a centralized Key Management Service (KMS).

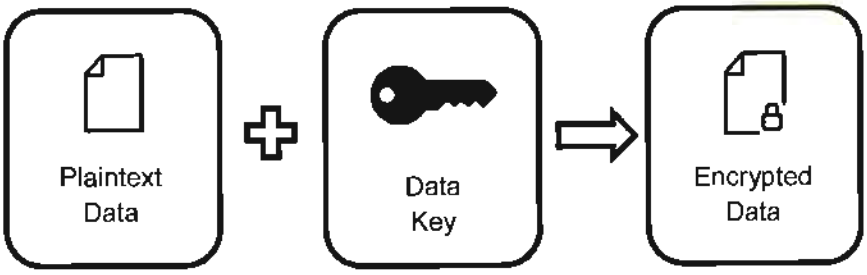
Envelope Encryption

Envelope encryption uses "Data keys" which are symmetric encryption keys along with "Key encrypting keys" which encrypt / decrypt the Data keys.

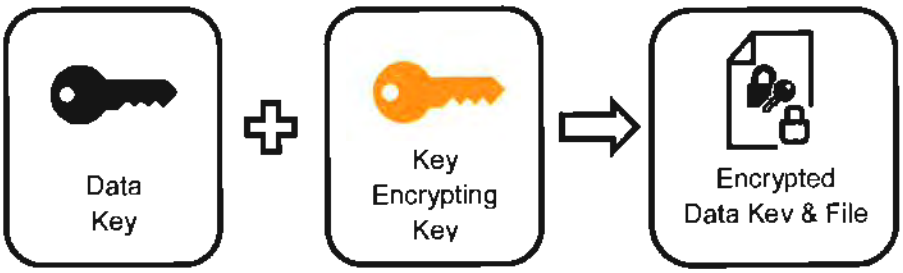
(1) Data key is generated to encrypt a file (one data key per file)



(2) Data key is used to encrypt the file



(3) Data key is encrypted using a Key-Encrypting key. The encrypted Data key is stored with the encrypted file. A plain text file header contains the Key-Encrypting key's Id.



Key Management

VisualVault encryption and decryption processing takes place within a Hardened Security Appliance (HSA).

Master keys are used to protect the Key-Encrypting keys used by the Envelope encryption process and are never exported from the HSA in plain text.

The result of the key management infrastructure is:

- Files may only be decrypted using the Hardware Security Appliance
- Each file is encrypted using a unique Data encryption key
- Data encryption keys are protected by Key Encrypting keys
- Key encrypting keys are only known to the Hardened Security Appliance and are managed by the Master keys.

Master keys stored within the HSA are rotated periodically such that a new master keys are generated and designated active; previously active master keys are marked as inactive. Inactive master keys may still be used by the key hierarchy for decryption. Each tenant may by assigned a unique Master key.

All access to the Hardened Security Appliance is logged by a centralized tamper proof logging system.

ISO 27001: IT Security

Information Security Incident Management - Management of Information Security Incidents and Improvements

TABLE OF CONTENTS

Section 13.2 Information Security Incident Management – Management of Information Security Incidents and Improvements

Introduction

Section 13.2 comprises of 13.2.1 Responsibilities and Procedure, 13.2.2 learning from Information Security Incidents and 13.2.3 Collection of Evidence.

13.2.1 Responsibilities and Procedures

It is the responsibility of the management and staff of an area where a security incident occurs to resolve the issue, test the resolution to insure that other areas are not compromised by the change, understand what happened and put in place work instructions or safe guard procedures to prevent future incidents. Personnel should develop ahead of time where possible contingency plans to resolve known security issues. Those contingency plans may include but are not limited to:

- Information System Failure or Loss of Service.
- Malicious Code
- Denial of Service
- Errors resulting from incomplete or inaccurate business data.
- Breaches of security, confidentiality, or integrity.
- Misuse of information systems or technology assets.

Maintenance should be maintained with high levels of response times for systems that are critical to the customer production environments up time.

Staff should meticulously record what has been reported about a security incident. They should also record what has been tried to resolve an issue and what the configurations of the system were before and after each change. When an incident's resolution is prolonged, management should develop an action plan to continue resolving the issue and advise staff of the plan. Staff should involve necessary external vendors quickly if the incident cannot be resolved in order to try and expedite a resolution.

If there is a breach of security affected customers must be notified by providing a written description of the incident to customer service for distribution to the affected customers.

13.2.2 Learning From Information Security Incidents

Once the issue is fully resolved, support request, procedures, configuration documents, and other pertinent documentation should be updated in order to record the knowledge gained from the incident. A security incident form must be submitted (security incident e-form available at https://na3.visualvault.com).

13.2.3 Collection of Evidence

When an incident has occurred it may become a legal matter; all event logs, audit trails, screen shots and pertinent information must be retained. A copy of the information should also be given to a Senior Executive. Under some circumstances if the evidence may lead to the termination of employment, that information should be given directly to the top Human Resources manager without tampering of the information. If the action may be against the top Human Resources manager, the information should be given to a Senior Executive. Refer to the company policies and procedures handbook and seek counsel from Human Resources as well as the President in relation to evidence leading to termination.

In the event that legal or termination actions are considered against any offending party, the company should measure the compliance of the system to the policies and procedures of the company to make sure they are in absolute compliance with any violations.

ISO 27001: IT Security

Information Security Incident Management Response Plan

TABLE OF CONTENTS

Information Security Incident Management - Response Plan

Introduction

Information Security Incident Management policies are documented in section 13.3 of the company security policies. This document represents the specific steps taken during an incident response.

It is the responsibility of the management and staff of an area where a security incident occurs to understand company security incident policies and follow this plan.

Security Incident detected or suspected Contact Procedure

Employees and Customers

1. **Contact VisualVault Support by sending an email to support@visualvault.com with a subject line containing the words "security incident".** Support staff use email filtering tags to provide an audible alert tone on their mobile devices based on the email containing this phrase.
2. **Contact VisualVault support phone number at 480-308-4400 option #2**
3. **If you are a support staff member you must follow step 1**
4. **If you are a customer, please provide all relevant contact information including mobile phone numbers and any relevant details**

Support Team

1. Verify the support ticket or support line caller provides all relevant information. If necessary ask for mobile phone numbers, incident details, date/time, etc.
2. Contact the Incident Response Team members listed in this document
3. Forward the support ticket information to the Incident Response Team members listed in this document.
4. Submit a Security Incident form with all relevant details and contact information after contacting the Incident Response Team.

Incident Response Team Procedures

Initial Assessment

1. Determine if the incident is real
    i. Collaborate with team members to review logs and examine evidence submitted. Make a determination if the incident is real or perceived.
2. If incident determined to be real, go to the Containment procedure

3. If incident is not real document the team's findings in the incident response form and notify submitter.

Containment

Team members will establish and follow one of the following procedures based on the initial assessment:

1. Virus response procedure
2. System failure procedure
3. Active intrusion response procedure - Is critical data at risk?
4. Inactive Intrusion response procedure
5. System abuse procedure
6. Property theft response procedure
7. Website DOS response procedure
8. Database or file denial of service response procedure
9. Malware response procedure
10. Customer data breach (includes specific procedures for PHI, and PCI data)
11. The team may create additional procedures which are not included in this document. If there is no applicable procedure in place, the team will document what was done and establish a procedure after the incident has been resolved.

Notification

1. The most senior member on the response team will determine notification protocol. In all cases the person reporting the incident must be notified of the status no later than completion of the containment procedures.
2. No employee is authorized to communicate with media, press, or any person outside of the response and support teams with the exception of the individuals who reported the incident.
3. The most senior member on the response team is responsible for notifying the executive team in the event of a customer data breach.
4. A member of the executive team is responsible for customer communication in the event of customer data breach.

Evidence Preservation

1. When an incident has occurred it may become a legal matter; all event logs, audit trails, screen shots and pertinent information must be retained. Under some circumstances if the evidence may lead to the termination of employment, that information should be given directly to a senior Executive without tampering. Refer to the company policies and procedures handbook and seek counsel from Human Resources in relation to evidence leading to termination.
2. In the event that legal or termination actions are considered against any offending party, the company should measure the compliance of the system to the policies and procedures of the company to make sure they are in absolute compliance with any violations.

3. Once the issue is fully resolved all evidence should be documented in the Security Incident Form

Security Incident Response Team Contact Information

Team Member	**Title**	**Mobile**	**Email**
Tod Olsen	CTO		
Wayne Hollingshead	Network Engineer		
Derrick Carlo	System Analyst		
Mike Betz	Support Manager		
Jeoff Camden	Senior Software Engineer		