

**State of Nebraska, Department of Health and Human Services  
REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES**

**RETURN TO:**

Name: René A. Botts/Carrie DeFreece  
Address: 301 Centennial Mall S, Suite 500  
City/State/Zip: Lincoln, NE 68509  
Phone: (402) 471-0727

<b>SOLICITATION NUMBER</b>	<b>RELEASE DATE</b>
RFP 113578 O3	October 18, 2022
<b>OPENING DATE AND TIME</b>	<b>PROCUREMENT CONTACT</b>
November 23, 2022, 2:00 p.m. Central Time	René A. Botts and Carrie DeFreece

**PLEASE READ CAREFULLY!  
SCOPE OF SERVICE**

The State of Nebraska (State), Department of Health and Human Services (DHHS), is issuing this Request for Proposal (RFP) Number 113578 O3 for the purpose of selecting a qualified Contractor to provide additional call center support services for ACCESSNebraska. A more detailed description can be found in Section V. The resulting contract may not be an exclusive contract as the State reserves the right to contract for the same or similar services from other sources now or in the future.

The term of the contract will be three (3) years commencing upon execution of the contract by the State and the Contractor (Parties). The Contract includes the option to renew for three (3) additional one (1) year periods upon mutual agreement of the Parties. The State reserves the right to extend the period of this contract beyond the termination date when mutually agreeable to the Parties.

ALL INFORMATION PERTINENT TO THIS REQUEST FOR PROPOSAL CAN BE FOUND ON THE INTERNET AT:  
<https://das.nebraska.gov/materiel/bidopps.html>.

**IMPORTANT NOTICE:** Pursuant to Neb. Rev. Stat. § 84-602.04, State contracts in effect as of January 1, 2014, and contracts entered into thereafter, must be posted to a public website. The resulting contract, the solicitation, and the awarded bidder's proposal and response will be posted to a public website managed by DAS, which can be found at <http://statecontracts.nebraska.gov> And [https://www.nebraska.gov/das/materiel/purchasing/contract\\_search/index.php](https://www.nebraska.gov/das/materiel/purchasing/contract_search/index.php).

In addition and in furtherance of the State's public records Statute (Neb. Rev. Stat. § 84-712 et seq.), all proposals or responses received regarding this solicitation will be posted to the State Purchasing Bureau public website.

These postings will include the entire proposal or response. Bidder must request that proprietary information be excluded from the posting. The bidder must identify the proprietary information, mark the proprietary information according to state law, and submit the proprietary information in a separate container or envelope marked conspicuously using an indelible method with the words "PROPRIETARY INFORMATION". The bidder should submit a detailed written document showing that the release of the proprietary information would give a business advantage to named business competitor(s) and explain how the named business competitor(s) will gain an actual business advantage by disclosure of information. The mere assertion that information is proprietary or that a speculative business advantage might be gained is not sufficient. (See Attorney General Opinion No. 92068, April 27, 1992) THE BIDDER MAY NOT ASSERT THAT THE ENTIRE PROPOSAL IS PROPRIETARY. COST PROPOSALS WILL NOT BE CONSIDERED PROPRIETARY AND ARE A PUBLIC RECORD IN THE STATE OF NEBRASKA. The State will determine, in its sole discretion, if the disclosure of the information designated by the Bidder as proprietary would 1) give advantage to business competitors and 2) serve no public purpose. The Bidder will be notified of the State's decision. Absent a determination by the State that the information may be withheld pursuant to Neb. Rev. Stat. § 84-712.05, the State will consider all information a public record subject to disclosure.

If the agency determines it is required to release proprietary information, the bidder will be informed. It will be the bidder's responsibility to defend the bidder's asserted interest in non-disclosure.

To facilitate such public postings, with the exception of proprietary information, the State of Nebraska reserves a royalty-free, nonexclusive, and irrevocable right to copy, reproduce, publish, post to a website, or otherwise use any contract, proposal, or response to this solicitation for any purpose, and to authorize others to use the documents. Any individual or entity awarded a contract, or who submits a proposal or response to this solicitation, specifically waives any copyright or other protection the contract, proposal, or response to the solicitation may have; and, acknowledges that they have the ability and authority to enter into such waiver. This reservation and waiver is a prerequisite for submitting a proposal or response to this solicitation, and award of a contract. Failure to agree to the reservation and waiver will result in the proposal or response to the solicitation being found non-responsive and rejected.

Any entity awarded a contract or submitting a proposal or response to the solicitation agrees not to sue, file a claim, or make a demand of any kind, and will indemnify and hold harmless the State and its employees, volunteers, agents, and its elected and appointed officials from and against any and all 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, sustained or asserted against the State, arising out of, resulting from, or attributable to the posting of the contract or the proposals and responses to the solicitation, awards, and other documents.**

# TABLE OF CONTENTS

REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES .....	i
TABLE OF CONTENTS .....	iii
GLOSSARY OF TERMS .....	v
ACRONYM LIST .....	viii
<b>I. PROCUREMENT PROCEDURE .....</b>	<b>1</b>
A. GENERAL INFORMATION .....	1
B. PROCURING OFFICE AND COMMUNICATION WITH STATE STAFF AND EVALUATORS .....	1
C. SCHEDULE OF EVENTS .....	2
D. WRITTEN QUESTIONS AND ANSWERS .....	3
E. SECRETARY OF STATE/TAX COMMISSIONER REGISTRATION REQUIREMENTS (Statutory) .....	3
F. ETHICS IN PUBLIC CONTRACTING .....	3
G. DEVIATIONS FROM THE REQUEST FOR PROPOSAL .....	3
H. SUBMISSION OF PROPOSALS .....	3
I. PROPOSAL PREPARATION COSTS .....	5
J. FAILURE TO COMPLY WITH REQUEST FOR PROPOSAL .....	5
K. PROPOSAL CORRECTIONS .....	5
L. LATE PROPOSALS .....	5
M. PROPOSAL OPENING .....	5
N. REQUEST FOR PROPOSAL/PROPOSAL REQUIREMENTS .....	5
O. EVALUATION COMMITTEE .....	6
P. EVALUATION OF PROPOSALS .....	6
Q. ORAL INTERVIEWS/PRESENTATIONS AND/OR DEMONSTRATIONS .....	7
R. BEST AND FINAL OFFER .....	7
S. REFERENCE AND CREDIT CHECKS .....	7
T. AWARD .....	7
U. ALTERNATE/EQUIVALENT PROPOSALS .....	8
V. LUMP SUM OR "ALL OR NONE" PROPOSALS .....	8
W. REJECTION OF PROPOSALS .....	9
X. RESIDENT BIDDER .....	9
<b>II. TERMS AND CONDITIONS .....</b>	<b>10</b>
A. GENERAL .....	10
B. NOTIFICATION .....	11
C. NOTICE (POC) .....	11
D. GOVERNING LAW (Statutory) .....	11
E. BEGINNING OF WORK .....	12
F. AMENDMENT .....	12
G. CHANGE ORDERS OR SUBSTITUTIONS .....	12
H. VENDOR PERFORMANCE REPORT(S) .....	13
I. NOTICE OF POTENTIAL CONTRACTOR BREACH .....	13
J. BREACH .....	13
K. NON-WAIVER OF BREACH .....	14
L. SEVERABILITY .....	14
M. INDEMNIFICATION .....	14
N. ATTORNEY'S FEES .....	15
O. ASSIGNMENT, SALE, OR MERGER .....	15
P. FORCE MAJEURE .....	16
Q. CONFIDENTIALITY .....	16
R. OFFICE OF PUBLIC COUNSEL (Statutory) .....	16
S. LONG-TERM CARE OMBUDSMAN (Statutory) .....	16
T. EARLY TERMINATION .....	16
U. CONTRACT CLOSEOUT .....	17

<b>III.</b>	<b>CONTRACTOR DUTIES.....</b>	<b>18</b>
A.	INDEPENDENT CONTRACTOR / OBLIGATIONS .....	18
B.	EMPLOYEE WORK ELIGIBILITY STATUS.....	19
C.	COMPLIANCE WITH CIVIL RIGHTS LAWS AND EQUAL OPPORTUNITY EMPLOYMENT / NONDISCRIMINATION (Statutory).....	19
D.	COOPERATION WITH OTHER CONTRACTORS.....	19
E.	DISCOUNTS.....	<b>Error! Bookmark not defined.</b>
F.	PRICES.....	<b>Error! Bookmark not defined.</b>
G.	COST CLARIFICATION .....	<b>Error! Bookmark not defined.</b>
H.	PERMITS, REGULATIONS, LAWS.....	20
I.	OWNERSHIP OF INFORMATION AND DATA / DELIVERABLES.....	20
J.	INSURANCE REQUIREMENTS .....	20
K.	NOTICE OF POTENTIAL CONTRACTOR BREACH .....	<b>Error! Bookmark not defined.</b>
L.	ANTITRUST.....	23
M.	CONFLICT OF INTEREST .....	23
N.	ADVERTISING.....	23
O.	NEBRASKA TECHNOLOGY ACCESS STANDARDS (Statutory) .....	23
P.	DISASTER RECOVERY/BACK UP PLAN.....	24
Q.	DRUG POLICY .....	24
R.	WARRANTY .....	24
S.	LOBBYING .....	24
T.	AMERICAN WITH DISABILITIES ACT.....	25
<b>IV.</b>	<b>PAYMENT.....</b>	<b>26</b>
A.	PROHIBITION AGAINST ADVANCE PAYMENT (Statutory).....	26
B.	TAXES (Statutory).....	26
C.	INVOICES .....	26
D.	INSPECTION AND APPROVAL .....	26
E.	PAYMENT (Statutory) .....	26
F.	LATE PAYMENT (Statutory).....	27
G.	SUBJECT TO FUNDING / FUNDING OUT CLAUSE FOR LOSS OF APPROPRIATIONS (Statutory).....	27
H.	RIGHT TO AUDIT (First Paragraph is Statutory) .....	27
<b>V.</b>	<b>PROJECT DESCRIPTION AND SCOPE OF WORK .....</b>	<b>28</b>
A.	PROJECT OVERVIEW .....	28
B.	PROJECT ENVIRONMENT.....	28
C.	SCOPE OF WORK .....	28
<b>VI.</b>	<b>PROPOSAL REQUIREMENTS.....</b>	<b>34</b>
A.	PROPOSAL SUBMISSION.....	34
<b>VII.</b>	<b>ATTACHMENTS .....</b>	<b>36</b>
	<b>Attachment 1 - Form A Contractor Proposal Point of Contact .....</b>	<b>37</b>
	<b>Attachment 2 - FORM B REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM .....</b>	<b>38</b>
	<b>Attachment 3 - Required Bidder Responses AccessNebraska</b>	
	<b>Attachment 4 - Cost Proposal Sheet</b>	
	<b>Attachment 5 - Sample Quality Assurance Form</b>	
	<b>Attachment 6 - Sample Quality Evaluation Scoring Report</b>	
	<b>Attachment 7 - Daily report Sample</b>	
	<b>Attachment 8 - Monthly Call Volume</b>	

## GLOSSARY OF TERMS

**Addendum:** Something to be added or deleted to an existing document; a supplement.

**After Receipt of Order (ARO):** After Receipt of Order.

**Agency:** Any state agency, board, or commission other than the University of Nebraska, the Nebraska State colleges, the courts, the Legislature, or any other office or agency established by the Constitution of Nebraska.

**Agent/Representative:** A person authorized to act on behalf of another.

**Amend:** To alter or change by adding, subtracting, or substituting.

**Amendment:** A written correction or alteration to a document.

**Appropriation:** Legislative authorization to expend public funds for a specific purpose. Money set apart for a specific use.

**Automated Clearing House: (ACH)** Electronic network for financial transactions in the United States

**Award:** All purchases, leases, or contracts which are based on competitive proposals will be awarded according to the provisions in the solicitation.

**Best and Final Offer (BAFO):** In a competitive proposal, the final offer submitted which contains the contractor's most favorable terms for price.

**Bid Bond:** An insurance agreement, accompanied by a monetary commitment, by which a third party (the surety) accepts liability and guarantees that the contractor will not withdraw the bid.

**Bidder:** A vendor who submits a proposal in response to a written solicitation.

**Breach:** Violation of a contractual obligation by failing to perform or repudiation of one's own promise.

**Business:** Any corporation, partnership, individual, sole proprietorship, joint-stock company, joint venture, or any other private legal entity.

**Business Day:** Any weekday, except State-recognized holidays.

**Calendar Day:** Every day shown on the calendar including Saturdays, Sundays, and State/Federal holidays.

**Cancellation:** To call off or revoke a purchase order or contract without expectation of conducting or performing it at a later time.

**Change Order:** Document that provides an addendum and/or amendments to an executed purchase order or contract.

**Collusion:** An agreement or cooperation between two or more persons or entities to accomplish a fraudulent, deceitful, or unlawful purpose.

**Competition:** The effort or action of two or more commercial interests to obtain the same business from third parties.

**Confidential Information:** Unless otherwise defined below, "Confidential Information" shall also mean proprietary trade secrets, academic and scientific research work which is in progress and unpublished, and other information which if released would give advantage to business competitors and serve no public purpose (see Neb. Rev. Stat. §84-712.05(3)). In accordance with Nebraska Attorney General Opinions 92068 and 97033, proof that information is proprietary requires identification of specific, named competitor(s) who would be advantaged by release of the information and the specific advantage the competitor(s) would receive.

**Contract:** An agreement between two or more parties creating obligations that are enforceable or otherwise recognizable at law; the writing that sets forth such an agreement.

**Contract Administration:** The administration of the contract which includes and is not limited to; contract signing, contract amendments and any necessary legal actions.

**Contract Award:** Occurs upon execution of the State document titled "Service Contract Award" by the proper authority.

**Contract Management:** The management of day-to-day activities at the agency which includes and is not limited to ensuring deliverables are received, specifications are met, handling meetings and making payments to the Contractor.

**Contract Period:** The duration of the contract.

**Contractor:** An individual or entity lawfully conducting business in the State, or licensed to do so, who seeks to provide goods or services under the terms of a written solicitation.

**Copyright:** A property right in an original work of authorship fixed in any tangible medium of expression, giving the holder the exclusive right to reproduce, adapt and distribute the work.

**Customer Service:** The process of ensuring customer satisfaction by providing assistance and advice on those products or services provided by the Contractor.

**Default:** The omission or failure to perform a contractual duty.

**Deviation:** Any proposed change(s) or alteration(s) to either the terms and conditions or deliverables within the scope of the written solicitation or contract.

**Evaluation:** The process of examining an offer after opening to determine the contractor's responsibility, responsiveness to requirements, and to ascertain other characteristics of the offer that relate to determination of the successful award.

**Evaluation Committee:** Individuals selected by the requesting agency for the evaluation of proposals (offers made in response to written solicitations).

**Extension:** Continuance of a contract for a specified duration upon the agreement of the parties beyond the original Contract Period. Not to be confused with "Renewal Period".

**Foreign Corporation:** A foreign corporation that was organized and chartered under the laws of another state, government, or country.

**Interested Party:** A person, acting in their personal capacity, or an entity entering into a contract or other agreement creating a legal interest therein.

**Invalid Proposal:** A proposal that does not meet the requirements of the solicitation or cannot be evaluated against the other proposals.

**Late Proposal:** An offer received after the Opening Date and Time.

**Mandatory/Must/Shall/Will:** Required, compulsory, or obligatory.

**May:** Discretionary, permitted; used to express possibility.

**Nebraska Family Online Client User System(N-Focus):** Nebraska's internal database.

**Non-Responsive Proposal:** Any proposal that does not comply with the requirements of the Request For Proposal.

**Opening Date and Time:** Specified date and time for the public opening of received, labeled, and sealed formal proposals.

**Performance Bond:** An insurance agreement, accompanied by a monetary commitment, by which a third party (the surety) accepts liability and guarantees that the Contractor fulfills any and all obligations under the contract.

**Point of Contact (POC):** The person designated to receive communications and to communicate.

**Project:** The total scheme, program, or method worked out for the accomplishment of an objective, including all documentation, commodities, and services to be provided under the contract.

**Proposal:** Bidder's response to a written solicitation.

**Proprietary Information:** Proprietary information is defined as trade secrets, academic and scientific research work which is in progress and unpublished, and other information which if released would give advantage to business competitors and serves no public purpose (see Neb. Rev. Stat. § 84-712.05(3)). In accordance with Attorney General Opinions 92068 and 97033, proof that information is proprietary requires identification of specific named competitor(s) advantaged by release of the information and the demonstrated advantage the named competitor(s) would gain by the release of information.

**Protest/Grievance:** A complaint about a governmental action or decision related to a solicitation or resultant contract, brought by a bidder who has submitted a proposal response by the opening date and time in connection with the award in question, to AS Materiel Division or another designated agency with the intention of achieving a remedial result.

**Public Proposal Opening:** The process of opening correctly submitted offers at the synchronous remote time and place specified in the written solicitation and in the virtual presence of anyone who wished to attend.

**Release Date:** The date of public release of the written solicitation to seek offers.

**Renewal Period:** Optional contract periods subsequent to the original Contract Period for a specified duration with previously agreed to terms and conditions. Not to be confused with Extension.

**Request for Proposal (RFP):** A written solicitation utilized for obtaining competitive offers.

**Responsible Contractor:** A contractor who has the capability in all respects to perform fully and lawfully all requirements with integrity and reliability to assure good faith performance.

**Responsive Bidder:** A bidder who has submitted a proposal which conforms to all requirements of the solicitation document.

**Shall/Will/Must:** An order/command; mandatory.

**Should:** Expected; suggested, but not necessarily mandatory.

**Specifications:** The detailed statement, especially of the measurements, quality, materials, and functional characteristics, or other items to be provided under a contract.

**Statutory:** These clauses are controlled by state law and are not subject to negotiation.

**Stop Order:** An order issued by the State to the contractor to stop all work.

**Subcontractor:** Individual or entity with whom the contractor enters a contract to perform a portion of the work awarded to the contractor.

**Termination:** Occurs when either Party, pursuant to a power created by agreement or law, puts an end to the contract prior to the stated expiration date. All obligations which are still executory on both sides are discharged but any right based on prior breach or performance survives.

**Third Party:** Any person or entity, including but not limited to fiduciaries, shareholders, owners, officers, managers, employees, legally disinterested persons, and sub-contractors or agents, and their employees. It shall not include any entity or person who is an interested Party to the contract or agreement.

**Trade Secret:** Information, including, but not limited to, a drawing, formula, pattern, compilation, program, device, method, technique, code, or process that (a) derives independent economic value, actual or potential, from not being known to, and not being ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy (see Neb. Rev. Stat. §87-502(4)).

**Trademark:** A word, phrase, logo, or other graphic symbol used by a manufacturer or contractor to distinguish its product from those of others, registered with the U.S. Patent and Trademark Office.

**Upgrade:** Any change that improves or alters the basic function of a product or service.

**Vendor Performance Report:** A report completed by the using agency and submitted to State Purchasing Bureau documenting products or services delivered or performed which exceed or fail to meet the terms of the purchase order, contract, and/or solicitation specifications.

**Vendor:** An individual or entity lawfully conducting business with the State.

**Will:** See Mandatory/Shall/Will/Must.

**Work Day:** See Business Day.

## ACRONYM LIST

**AABD** – Aid- to Aged, Blind and Disabled

**ACD** – Automatic Call Distribution

**AHT** – Average Handle Time

**ADC** – Aid to Dependent Children

**ANI** – Automatic Number Identification

**ARO** – After Receipt of Order

**ASA** – Average Speed of Answer

**ACH** – Automated Clearing House

**BAFO** – Best and Final Offer

**CMS** – Centers for Medicare and Medicaid Services

**CRM** – Customer Relationship Management

**CSC** – Customer Service Centers

**COI** – Certificate of Insurance

**DAS** – Department of Administrative Services

**DHHS** – Department of Health and Human Services

**EBT** – Electronic Benefit Transfer

**HIPAA** – Health Insurance Portability and Accountability Act

**LIHEAP** – Low Income Home Energy Assistance Program

**MC** – Master Case

**N-Focus** -- Nebraska's internal database.

**NITC** – Nebraska Information Technology Commission

**PHI** – Personal Health Information

**PII** – Personal Identifying Information

**QA** – Quality Assurance

**RFP** – Request for Proposal

**SNAP** – Supplemental Nutrition Assistance Program

**SPB** – State Purchasing Bureau

**SSAD** – Social Services for the Aged and Disabled

**SSN** – Social Security Number



## I. PROCUREMENT PROCEDURE

### A. GENERAL INFORMATION

The solicitation is designed to solicit proposals from qualified bidder who will be responsible for providing additional call center support services for ACCESSNebraska at a competitive and reasonable cost. Terms and Conditions, Project Description and Scope of Work, Proposal instructions, and Cost Proposal Requirements may be found in Sections II through VII.

Proposals shall conform to all instructions, conditions, and requirements included in the solicitation. Prospective bidders are expected to carefully examine all documents, schedules, and requirements in this solicitation, and respond to each requirement in the format prescribed. Proposals may be found non-responsive if they do not conform to the solicitation.

### B. PROCURING OFFICE AND COMMUNICATION WITH STATE STAFF AND EVALUATORS

Procurement responsibilities related to this solicitation reside with the Department of Health and Human Services. The points of contact (POC) for the procurement are as follows:

Name: René A. Botts and Carrie DeFreece  
Agency: Department of Health and Human Services  
Address: 301 Centennial Mall South, Suite 500  
Lincoln, NE 68509

Telephone: 402-471-0727

E-Mail: [dhhs.rfpquestions@nebraska.gov](mailto:dhhs.rfpquestions@nebraska.gov)

From the date the solicitation is issued until the Intent to Award is issued, communication from the bidder is limited to the POCs listed above. After the Intent to Award is issued, the bidder may communicate with individuals the State has designated as responsible for negotiating the contract on behalf of the State. No member of the State Government, employee of the State, or member of the Evaluation Committee is empowered to make binding statements regarding this solicitation. The POCs will issue any answers, clarifications or amendments regarding this solicitation in writing. Only DHHS can award a contract for this RFP. Bidders shall not have any communication with or attempt to communicate or influence any evaluator involved in this solicitation.

The following exceptions to these restrictions are permitted:

1. Contact made pursuant to pre-existing contracts or obligations;
2. Contact required by the schedule of events or an event scheduled later by the solicitation POC; and
3. Contact required for negotiation and execution of the final contract.

*The State reserves the right to reject a bidder's proposal, withdraw an Intent to Award, or terminate a contract if the State determines there has been a violation of these procurement procedures.*

**C. SCHEDULE OF EVENTS**

The State expects to adhere to the procurement schedule shown below, but all dates are approximate and subject to change.

ACTIVITY	DATE/TIME
1. Release Solicitation	October 18, 2022
2. Last day to submit written questions	November 1, 2022
3. State responds to written questions through Solicitation "Addendum" and/or "Amendment" to be posted to the Internet at: <a href="https://das.nebraska.gov/materiel/bidopps.html">https://das.nebraska.gov/materiel/bidopps.html</a>	November 8, 2022
<p>Proposal Opening via WebEx:</p> <div data-bbox="318 537 688 630" style="background-color: #008000; color: white; text-align: center; padding: 10px; margin: 10px 0;"> <p style="font-size: 1.2em; margin: 0;">Join meeting</p> </div> <p><b>More ways to join:</b></p> <p><b>Join from the meeting link</b>  <a href="https://sonvideo.webex.com/sonvideo/j.php?MTID=m907cc048d0">https://sonvideo.webex.com/sonvideo/j.php?MTID=m907cc048d0</a></p> <p><b>Join by meeting number</b>            Meeting number (access code): 2482 094 7978            Meeting password: YYiHw4mpB23</p> <p><b>Join by phone</b>            +1-408-418-9388 United States Toll  <a href="#">Global call-in numbers</a></p> <p><b>Join from a video system or application</b>            Dial <a href="tel:24820947978">24820947978@sonvideo.webex.com</a>            You can also dial 173.243.2.68 and enter your meeting number.</p> <p><b>Join using Microsoft Lync or Microsoft Skype for Business</b>            Dial <a href="tel:24820947978">24820947978.sonvideo@lync.webex.com</a>            Need help? Go to <a href="https://help.webex.com">https://help.webex.com</a></p>	<p>November 23, 2022            2:00 PM            Central Time</p>
5. Review for conformance to solicitation requirements	November 28, 2022
6. Evaluation period	November 28, 2022 – December 8, 2022
7. "Oral Interviews/Presentations and/or Demonstrations" (if required)	TBD
8. Post "Notification of Intent to Award" to Internet at: <a href="https://das.nebraska.gov/materiel/bidopps.html">https://das.nebraska.gov/materiel/bidopps.html</a>	December 9, 2022
9. Contract finalization period	December 9, 2022 – January 9, 2023
10. Contract award	January 13, 2023
11. Contractor start date	January 23, 2023

**D. WRITTEN QUESTIONS AND ANSWERS**

Questions regarding the meaning or interpretation of any solicitation provision must be submitted in writing to DHHS and clearly marked "RFP Number 113578 O3; Call center support services for ACCESSNebraska Questions". The POCs are not obligated to respond to questions that are received late per the Schedule of Events.

Bidders should present, as questions, any assumptions upon which the Bidder's proposal is or might be developed. **Any proposal containing assumptions may be deemed non-responsive. Non-responsive proposals may be rejected by the State.** Proposals will be evaluated without consideration of any known or unknown assumptions of a bidder. The contract will not incorporate any known or unknown assumptions of a bidder.

It is preferred that questions be sent via e-mail to [dhhs.rfpquestions@nebraska.gov](mailto:dhhs.rfpquestions@nebraska.gov), but may be delivered by hand or by U.S. Mail. It is recommended that Bidders submit questions using the following format.

Solicitation Section Reference	Solicitation Page Number	Question

Written answers will be posted at <https://das.nebraska.gov/materiel/bidopps.html> per the Schedule of Events.

**E. SECRETARY OF STATE/TAX COMMISSIONER REGISTRATION REQUIREMENTS (Statutory)**

All bidders must be authorized to transact business in the State of Nebraska and comply with all Nebraska Secretary of State Registration requirements. The bidder who is the recipient of an Intent to Award may be required to certify that it has complied and produce a true and exact copy of its current (within ninety (90) calendar days of the intent to award) Certificate or Letter of Good Standing, or in the case of a sole proprietorship, provide written documentation of sole proprietorship and complete the United States Citizenship Attestation Form, available on the Department of Administrative Services website at [Attestation form link](#). This must be accomplished prior to execution of the contract.

**F. ETHICS IN PUBLIC CONTRACTING**

The State reserves the right to reject proposals, withdraw an award or intent to award or award, or terminate a contract if a bidder or contractor commits or has committed ethical violations, which include, but are not limited to:

1. Offering or giving, directly or indirectly, a bribe, fee, commission, compensation, gift, gratuity, or anything of value to any person or entity in an attempt to influence the bidding process;
2. Utilize the services of lobbyists, attorneys, political activists, or consultants to influence or subvert the bidding process;
3. Being considered for, presently being, or becoming debarred, suspended, ineligible, or excluded from contracting with any state or federal entity;
4. Submitting a proposal on behalf of another Party or entity; and
5. Collude with any person or entity to influence the bidding process, submit sham proposals, preclude bidding, fix pricing or costs, create an unfair advantage, subvert the proposal, or prejudice the State.

The Contractor shall include this clause in any subcontract entered into for the exclusive purpose of performing this contract.

Bidder shall have an affirmative duty to report any violations of this clause by the Bidder throughout the bidding process, and throughout the term of this contract for the successful Contractor and their subcontractors.

**G. DEVIATIONS FROM THE REQUEST FOR PROPOSAL**

The requirements contained in the solicitation (Sections II thru VI) become a part of the terms and conditions of the contract resulting from this solicitation. Any deviations from the solicitation in Sections II through VI must be clearly defined by the bidder in its proposal and, if accepted by the State, will become part of the contract. Any specifically defined deviations must not be in conflict with the basic nature of the solicitation, requirements, or applicable state or federal laws or statutes. "Deviation", for the purposes of this solicitation, means any proposed changes or alterations to either the contractual language or deliverables within the scope of this solicitation. The State discourages deviations and reserves the right to reject proposed deviations.

**H. SUBMISSION OF PROPOSALS**

The State is accepting either electronically submitted responses or hard copy, paper responses for this RFP.

For bidders submitting electronic responses:

1. Bidders submitting electronically can upload the response via ShareFile here:

- a. <https://nebraska.sharefile.com/r-r5c5f56805d174eed827b3bcda9a113d5>
- b. ShareFile works with Firefox, Internet Explorer and Chrome. It does not work with Microsoft Edge.

2. The Cost Proposal and Proprietary information should be uploaded as separate and distinct files. If multiple proposals are submitted, the State will retain only the most recently submitted response. It is the bidder's responsibility to submit the proposal by the date and time indicated in the Schedule of Events. Electronic proposals must be received by DHHS by the date and time of the proposal opening per the Schedule of Events. No late proposals will be accepted

### 3. ELECTRONIC PROPOSAL FILE NAMES

The bidder should clearly identify the uploaded RFP proposal files. To assist in identification please use the following naming convention:

- a. RFP 113578 O3 ABC Company
- b. If multiple files are submitted for one RFP proposal, add number of files to file names: RFP 113578 O3 ABC Company File 1 of 2.
- c. If multiple RFP proposals are submitted for the same RFP, add the proposal number to the file names: RFP 113578 O3 ABC Company Proposal 1 File 1 of 2.

For bidders submitting paper/hard copy responses:

4. Bidders who are submitting a paper response should submit one proposal marked on the first page: "ORIGINAL". If multiple proposals are submitted, the State will retain one copy marked "ORIGINAL" and destroy the other copies. The Bidder is solely responsible for any variance between the copies submitted. Proposal responses should include the completed Form A, "Bidder Proposal Point of Contact". Proposals must reference the RFP number and be sent to the specified address. Please note that the address label should appear as specified in Section I B. on the face of each container or bidder's proposal response packet. If a recipient phone number is required for delivery purposes, 402-471-0524 should be used. The RFP number should be included in all correspondence. The State will not furnish packaging and sealing materials. It is the bidder's responsibility to ensure the solicitation is received in a sealed envelope or container and submitted by the date and time indicated in the Schedule of Events. Sealed proposals must be received in the State Purchasing Bureau by the date and time of the proposal opening per the Schedule of Events. No late proposals will be accepted.

United States Postal Services (USPS) delivered proposal responses shall be mailed to:

ATTN: René A. Botts/Carrie DeFreece RFP 113578 O3  
DHHS - Central Procurement Services  
PO BOX 94926  
Lincoln, NE 68509

Hand delivered proposal responses or responses delivered by Federal Express (FedEx), United Parcel Service (UPS), etc. shall be delivered to:

ATTN: René A. Botts/Carrie DeFreece RFP 113578 O3  
DHHS – 5th Floor HR Reception Desk  
301 Centennial Mall South  
Lincoln, NE 68509

5. The Cost Proposal and Proprietary Information should be presented in separate sections (loose-leaf binders are preferred) on standard 8 ½" x 11" paper, except that charts, diagrams and the like may be on fold-outs which, when folded, fit into the 8 ½" by 11" format. Pages may be consecutively numbered for the entire proposal, or may be numbered consecutively within sections. Figures and tables should be numbered consecutively within sections. Figures and tables should be numbered and referenced in the text by that number. They should be placed as close as possible to the referencing text.

Bidder must use the State's Cost Proposal Form.

The State will not furnish packaging or sealing materials. It is the bidder's responsibility to ensure the solicitation is received either electronically or in a sealed envelope or container and submitted by the date and time indicated in the Schedule of Events. Sealed proposals must be received in the State Purchasing Bureau by the date and time of the proposal opening per the Schedule of Events.

The Request for Proposal form must be signed in an indelible manner or by DocuSign and returned by the proposal opening date and time along with the bidder's Request for Proposal along with any other requirements as stated in the Request for Proposal document in order for the bidder's Request for Proposal response to be evaluated.

It is the responsibility of the bidder to check the website for all information relevant to this Request for Proposal to include addenda and/or amendments issued prior to the opening date. Website address is as follows: <https://das.nebraska.gov/materiel/bidopps.html>.

Emphasis should be concentrated on conformance to the solicitation instructions, responsiveness to requirements, completeness, and clarity of content. If the bidder's proposal is presented in such a fashion that makes evaluation difficult or overly time consuming the State reserves the right to reject the proposal as non-conforming.

The State shall not incur any liability for any costs incurred by bidders in replying to this solicitation, in the demonstrations and/or oral presentations, or in any other activity related to bidding on this solicitation.

By signing the "Request for Proposal for Contractual Services" form, the bidder guarantees compliance with the provisions stated in this solicitation.

**I. PROPOSAL PREPARATION COSTS**

The State shall not incur any liability for any costs incurred by Bidders in replying to this solicitation, including any activity related to bidding on this solicitation.

**J. FAILURE TO COMPLY WITH REQUEST FOR PROPOSAL**

Violation of the terms and conditions contained in this solicitation or any resultant contract, at any time before or after the award, shall be grounds for action by the State which may include, but is not limited to, the following:

1. Rejection of a bidder's proposal;
2. Withdrawal of the Intent to Award;
3. Withdrawal of the Award;
4. Negative Vendor Performance Report(s)
5. Termination of the resulting contract;
6. Legal action; and
7. Suspension of the bidder from further bidding with the State for the period of time relative to the seriousness of the violation, such period to be within the sole discretion of the State.

**K. PROPOSAL CORRECTIONS**

A bidder may correct a mistake in a proposal prior to the time of opening by uploading a revised and completed proposal if the original proposal was electronically submitted.

1. If a corrected electronic proposal is submitted, the file name(s) date/time stamped with latest date/time stamp will be accepted. The corrected proposal file name(s) should be identified as
  - a. Corrected 113578 O3 Company Name Proposal #1 Description of Service, File 1 of 2
  - b. Corrected 113578 O3 Company Name Proposal #2 Description of Service, File 2 of 2, etc.

Changing a proposal after opening may be permitted if the change is made to correct a minor error that does not affect price, quantity, quality, delivery, or contractual conditions. In case of a mathematical error in extension of price, unit price shall govern.

**L. LATE PROPOSALS**

Proposals received after the time and date of the proposal opening will be considered late proposals. Late proposals will be returned unopened, if requested by the bidder and at bidder's expense. The State is not responsible for proposals that are late or lost regardless of cause or fault.

**M. PROPOSAL OPENING**

The opening of proposals will be public and the bidders will be announced. Proposals **WILL NOT** be available for viewing by those present at the proposal opening. Proposals will be posted to the State Purchasing Bureau website once an Intent to Award has been posted to the website. Once proposals are opened, they become the property of the State of Nebraska and will not be returned.

**N. REQUEST FOR PROPOSAL/PROPOSAL REQUIREMENTS**

The proposals will first be examined to determine if all requirements listed below have been addressed and whether further evaluation is warranted. Proposals not meeting the requirements may be rejected as non-responsive. The requirements are:

1. Original Attachment 2 – Form B Request for Proposal for Contractual Services form signed manually in ink or by DocuSign;
2. Clarity and responsiveness of the proposal;
3. Completed Corporate Overview;
4. Completed Sections II through VII;
5. Attachment 3 – Required Bidder Responses;
6. Completed Solution Approach; and
7. Completed State Cost Proposal Template.

**O. EVALUATION COMMITTEE**

Proposals are evaluated by members of an Evaluation Committee(s). The Evaluation Committee(s) will consist of individuals selected at the discretion of the State. Names of the members of the Evaluation Committee(s) will not be published prior to the intent to award.

Any contact, attempted contact, or attempt to influence an evaluator that is involved with this solicitation may result in the rejection of this proposal and further administrative actions.

**P. EVALUATION OF PROPOSALS**

All proposals that are responsive to the solicitation will be evaluated. Each evaluation category will have a maximum point potential. The State will conduct a fair, impartial, and comprehensive evaluation of all proposals in accordance with the criteria set forth below. Areas that will be addressed and scored during the evaluation include:

1. Corporate Overview should include but is not limited to:
  - a. the ability, capacity, and skill of the bidder to deliver and implement the system or project that meets the requirements of the solicitation;
  - b. the character, integrity, reputation, judgment, experience, and efficiency of the bidder;
  - c. whether the bidder can perform the contract within the specified time frame;
  - d. the quality of vendor performance on prior contracts;
  - e. such other information that may be secured and that has a bearing on the decision to award the contract;
2. Solution Approach;
3. Required Bidder Responses; and,
4. Cost Proposal.

**Neb. Rev. Stat. §81-161 allows the quality of performance of previous contracts to be considered when evaluating responses to competitively bid solicitations in determining the lowest responsible bidder.** Information obtained from any Vendor Performance Report (See Terms & Conditions) may be used in evaluating responses to solicitations for goods and services to determine the best value for the State.

**Neb. Rev. Stat. §73-107 allows for a preference for a resident disabled veteran or business located in a designated enterprise zone.** When a state contract is to be awarded to the lowest responsible contractor, a resident disabled veteran or a business located in a designated enterprise zone under the Enterprise Zone Act shall be allowed a preference over any other resident or nonresident contractor, if all other factors are equal.

**Resident disabled veterans means any person (a) who resides in the State of Nebraska, who served in the United States Armed Forces, including any reserve component or the National Guard, who was discharged or otherwise separated with a characterization of honorable or general (under honorable conditions), and who possesses a disability rating letter issued by the United States Department of Veterans Affairs establishing a service-connected disability or a disability determination from the United States Department of Defense and (b)(i) who owns and controls a business or, in the case of a publicly owned business, more than fifty percent of the stock is owned by one or more persons described in subdivision (a) of this subsection and (ii) the management and daily business operations of the business are controlled by one or more persons described in subdivision(a) of this subsection. Any contract entered into without compliance with this section shall be null and void.**

Therefore, if a resident disabled veteran or business located in a designated enterprise zone submits a proposal in accordance with Neb. Rev. Stat. §73-107 and has so indicated on the solicitation cover page under “Bidder must complete the following” requesting priority/preference to be considered in the award of this contract, the following will need to be submitted by the contractor within ten (10) business days of request:

1. Documentation from the United States Armed Forces confirming service;

2. Documentation of discharge or otherwise separated characterization of honorable or general (under honorable conditions);
3. Disability rating letter issued by the United States Department of Veterans Affairs establishing a service-connected disability or a disability determination from the United States Department of Defense; and
4. Documentation which shows ownership and control of a business or, in the case of a publicly owned business, more than fifty percent of the stock is owned by one or more persons described in subdivision (a) of this subsection; and the management and daily business operations of the business are controlled by one or more persons described in subdivision (a) of this subsection.

Failure to submit the requested documentation within ten (10) business days of notice will disqualify the bidder from consideration of the preference.

Evaluation criteria will be released with the solicitation.

**Q. ORAL INTERVIEWS/PRESENTATIONS AND/OR DEMONSTRATIONS**

The State may determine after the completion of the Solution and Cost Proposal evaluation that oral interviews/presentations and/or demonstrations are required. Every bidder may not be given an opportunity to interview/present and/or give demonstrations; the State reserves the right, in its discretion, to select only the top scoring bidders to present/give oral interviews. The scores from the oral interviews/presentations and/or demonstrations will be added to the scores from the Solution and Cost Proposals. The presentation process will allow the bidders to demonstrate their proposal offering, explaining and/or clarifying any unusual or significant elements related to their proposals. Bidders' key personnel, identified in their proposal, may be requested to participate in a structured interview to determine their understanding of the requirements of this proposal, their authority and reporting relationships within their firm, and their management style and philosophy. Only representatives of the State and the presenting bidder will be permitted to attend the oral interviews/presentations and/or demonstrations. A written copy or summary of the presentation, and demonstrative information (such as briefing charts, et cetera) may be offered by the bidder, but the State reserves the right to refuse or not consider the offered materials. Bidders shall not be allowed to alter or amend their proposals.

Once the oral interviews/presentations and/or demonstrations have been completed, the State reserves the right to make an award without any further discussion with the bidders regarding the proposals received.

Any cost incidental to the oral interviews/presentations and/or demonstrations shall be borne entirely by the bidder and will not be compensated by the State.

**R. BEST AND FINAL OFFER**

If best and final offers (BAFO) are requested by the State and submitted by the contractor, they will be evaluated (using the stated BAFO criteria), scored, and ranked by the Evaluation Committee. The State reserves the right to conduct more than one Best and Final Offer. The award will then be granted to the highest scoring bidder. However, a bidder should provide its best offer in its original proposal. Bidders should not expect that the State will request a best and final offer.

**S. REFERENCE AND CREDIT CHECKS**

The State reserves the right to conduct and consider reference and credit checks. The State reserves the right to use third parties to conduct reference and credit checks. By submitting a proposal in response to this solicitation, the bidder grants to the State the right to contact or arrange a visit in person with any or all of the bidder's clients. Reference and credit checks may be grounds to reject a proposal, withdraw an intent to award, or rescind the award of a contract.

**T. AWARD**

The State reserves the right to evaluate proposals and award contracts in a manner utilizing criteria selected at the State's discretion and in the State's best interest. After evaluation of the proposals, or at any point in the solicitation process, the State of Nebraska may take one or more of the following actions:

1. Amend the solicitation;
2. Extend the time of or establish a new proposal opening time;
3. Waive deviations or errors in the State's solicitation process and in bidder proposals that are not material, do not compromise the solicitation process or a bidder's proposal, and do not improve a bidder's competitive position;
4. Accept or reject a portion of or all of a proposal;
5. Accept or reject all proposals;
6. Withdraw the solicitation;
7. Elect to rebid the solicitation;

8. Award single lines or multiple lines to one or more bidders; or,
9. Award one or more all-inclusive contracts.

The State of Nebraska may consider, but is not limited to considering, one or more of the following award criteria:

1. Price;
2. Location;
3. Quality;
4. Delivery time;
5. Contractor qualifications and capabilities; and
6. State contract management requirements and/or costs.

The solicitation does not commit the State to award a contract. Once intent to award decision has been determined, it will be posted to the Internet at:

<https://das.nebraska.gov/materiel/bidopps.html>

Any protests must be filed by a bidder within ten (10) business days after the intent to award decision is posted to the Internet. Grievance and protest procedure is available on the Internet at:

<https://dhhs.ne.gov/Guidance%20Docs/DHHS%20Grievance-Protest%20Procedures%20for%20Vendors.pdf>

**U. ALTERNATE/EQUIVALENT PROPOSALS**

Bidder may offer proposals which are at variance from the express specifications of the solicitation. The State reserves the right to consider and accept such proposals if, in the judgment of the Materiel Administrator, the proposal will result in goods and/or services equivalent to or better than those which would be supplied in the original proposal specifications. Bidder must indicate on the solicitation the manufacturer's name, number and shall submit with their proposal, sketches, descriptive literature and/or complete specifications. Reference to literature submitted with a previous proposal will not satisfy this provision. Proposals which do not comply with these requirements are subject to rejection. In the absence of any stated deviation or exception, the proposal will be accepted as in strict compliance with all terms, conditions and specification, and the Bidder shall be held liable therefore.

**V. LUMP SUM OR "ALL OR NONE" PROPOSALS**

The State reserves the right to purchase item-by-item, by groups or as a total when the State may benefit by so doing. Bidders may submit a proposal on an "all or none" or "lump sum" basis, but should also submit a proposal on an item-by-item basis. The term "all or none" means a conditional proposal which requires the purchase of all items on which proposals are offered and Bidder declines to accept award on individual items; a "lump sum" proposal is one in which the Bidder offers a lower price than the sum of the individual proposals if all items are purchased, but agrees to deliver individual items at the prices quoted.

**W. DISCOUNTS**

Prices quoted shall be inclusive of ALL trade discounts. Cash discount terms of less than thirty (30) days will not be considered as part of the proposal. Cash discount periods will be computed from the date of receipt of a properly executed claim voucher or the date of completion of delivery of all items in a satisfactory condition, whichever is later.

**X. PRICES**

Prices quoted shall be net, including transportation and delivery charges fully prepaid by the contractor, F.O.B. destination named in the solicitation. No additional charges will be allowed for packing, packages, or partial delivery costs. When an arithmetic error has been made in the extended total, the unit price will govern.

All prices, costs, and terms and conditions submitted in the proposal shall remain fixed and valid commencing on the opening date of the proposal until an award is made or the solicitation is cancelled.

Prices submitted on the cost proposal form shall remain fixed for the first twelve (12) months of the contract. The contractor may request a price increase no more than once per year subsequent to the first twelve (12) months of the contract. Once the increase is approved by DHHS, increases will be cumulative across the remaining periods of the contract. Requests for an increase must be submitted in writing to DHHS a minimum of 120 days prior to the effective date of the increase. Documentation will be required by DHHS to support the price increase.

**DHHS reserves the right to deny any requested price increase. No price increases are to be billed to DHHS prior to written amendment of the contract by the parties.**

**DHHS will be given full proportionate benefit of any decreases for the term of the contract.**



**Y. COST CLARIFICATION**

The State reserves the right to review all aspects of cost for reasonableness and to request clarification of any proposal where the cost component shows significant and unsupported deviation from industry standards or in areas where detailed pricing is required.

**Z. REJECTION OF PROPOSALS**

The State reserves the right to reject any or all proposals, wholly or in part, in the best interest of the State.

**AA. RESIDENT BIDDER**

Pursuant to Neb. Rev. Stat. §§ 73-101.01 through 73-101.02, a Resident Bidder shall be allowed a preference against a Non-resident Bidder from a state which gives or requires a preference to Bidders from that state. The preference shall be equal to the preference given or required by the state of the Nonresident Bidders. Where the lowest responsible bid from a resident Bidder is equal in all respects to one from a nonresident Bidder from a state which has no preference law, the resident Bidder shall be awarded the contract. The provision of this preference shall not apply to any contract for any project upon which federal funds would be withheld because of the provisions of this preference.

**II. TERMS AND CONDITIONS**

**Bidders should complete Sections II through VII as part of their proposal.** Bidder should 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 solicitation, 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 solicitation. The State of Nebraska reserves the right to reject proposals that attempt to substitute the bidder's commercial contracts and/or documents for this solicitation.

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.

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 Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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

1. Request for Proposal and Addenda;
2. Amendments to the solicitation;
3. Questions and Answers;
4. Contractor's proposal (Contractor's response to the solicitation and properly submitted documents); and
5. 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 solicitation and any Questions and Answers, 4) the original solicitation 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 Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

Bidder 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 five (5) calendar days following deposit in the mail.

Either party may change its address for notification purposes by giving notice of the change, and setting forth the new address and an effective date.

**C. NOTICE (POC)**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

The State reserves the right to appoint a Contract Manager to manage the contract on behalf of the State. The Contract Manager will be appointed in writing, and the appointment document will specify the extent of the Contract Manager authority and responsibilities. If a Contract Manager is appointed, the Contractor will be notified, and is expected to cooperate accordingly with the Contract Manager. The Contract Manager has no authority to bind the State to a contract, amendment, addendum, or other change or addition to the contract.

**D. 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.

**E. BEGINNING OF WORK**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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

**F. AMENDMENT**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

This Contract may be amended in writing, within scope, upon the agreement of both parties.

**G. CHANGE ORDERS OR SUBSTITUTIONS**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

The State and the Contractor, upon the written agreement, may make changes to the contract within the general scope of the solicitation. 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.

The Contractor shall prepare a written description of the work required due to the change and an itemized cost proposal sheet for the change. 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.

In the event any product is discontinued or replaced upon mutual consent during the contract period or prior to delivery, the State reserves the right to amend the contract or purchase order to include the alternate product at the same price.

**\*\*\*Contractor will not substitute any item that has been awarded without prior written approval of DHHS\*\*\***

**H. VENDOR PERFORMANCE REPORT(S)**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

The State may document any instance(s) of products or services delivered or performed which exceed or fail to meet the terms of the purchase order, contract, and/or solicitation specifications. The State Purchasing Bureau may contact the Vendor regarding any such report. Vendor performance report(s) will become a part of the permanent record of the Vendor.

**I. NOTICE OF POTENTIAL CONTRACTOR BREACH**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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.

**J. BREACH**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

Either Party may terminate the contract, in whole or in part, if the other Party breaches its duty to perform its obligations under the contract in a timely and proper manner. Termination requires written notice of default and a thirty (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 may recover from the Contractor as damages the difference between the costs of covering the breach. Notwithstanding any clause to the contrary, the State may also recover the contract price together with any incidental or consequential damages defined in UCC Section 2-715, but less expenses saved in consequence of Contractor's breach.

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

**K. NON-WAIVER OF BREACH**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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.

**L. SEVERABILITY**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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.

**M. INDEMNIFICATION**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

**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 solicitation.

**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 (§ 81-8,294), Tort (§ 81-8,209), and Contract Claim Acts (§ 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.

**N. ATTORNEY'S FEES**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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 ordered by the court, including attorney's fees and costs, if the other Party prevails.

**O. ASSIGNMENT, SALE, OR MERGER**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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.

**P. FORCE MAJEURE**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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.

**Q. CONFIDENTIALITY**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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.

**R. 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.

**S. LONG-TERM CARE OMBUDSMAN (Statutory)**

Contractor must comply with the Long-Term Care Ombudsman Act, per Neb. Rev. Stat. §§ 81-2237 et seq. This section shall survive the termination of this contract.

**T. EARLY TERMINATION**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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.

**U. CONTRACT CLOSEOUT**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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.

**III. CONTRACTOR DUTIES**

**A. INDEPENDENT CONTRACTOR / OBLIGATIONS**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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;
5. Determining the hours to be worked and the duties to be performed by the Contractor's employees; and,
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 contractor'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 Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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 [https://das.nebraska.gov/materiel/purchase\\_bureau/vendor-info.html](https://das.nebraska.gov/materiel/purchase_bureau/vendor-info.html)
2. The completed United States Attestation Form should be submitted with the solicitation response.
3. 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.
4. 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 goods and services to be covered by any contract resulting from this solicitation.

**D. COOPERATION WITH OTHER CONTRACTORS**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

Contractor may be required to work with 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 Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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 Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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 Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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 contractors' 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**

The Contractor shall take out and maintain during the life of this contract such Commercial General 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.**

<b>REQUIRED INSURANCE COVERAGE</b>		
<b>COMMERCIAL GENERAL LIABILITY</b>		
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
XCU Liability (Explosion, Collapse, and Underground Damage)		Included
Independent Contractors		Included
Abuse & Molestation		Included
<i>If higher limits are required, the Umbrella/Excess Liability limits are allowed to satisfy the higher limit.</i>		
<b>WORKER'S COMPENSATION</b>		
Employers Liability Limits		\$500K/\$500K/\$500K
Statutory Limits- All States		Statutory - State of Nebraska
USL&H Endorsement		Statutory
Voluntary Compensation		Statutory
<b>UMBRELLA/EXCESS LIABILITY</b>		
Over Primary Insurance		\$5,000,000 per occurrence
<b>COMMERCIAL CRIME</b>		
Crime/Employee Dishonesty Including 3rd Party Fidelity		\$1,000,000
<b>CYBER LIABILITY</b>		
Breach of Privacy, Security Breach, Denial of Service, Remediation, Fines and Penalties		\$10,000,000
<b>MANDATORY COI SUBROGATION WAIVER LANGUAGE</b>		
"Workers' Compensation policy shall include a waiver of subrogation in favor of the State of Nebraska."		
<b>MANDATORY COI LIABILITY WAIVER LANGUAGE</b>		
"Commercial General Liability & policy 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."		

### 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.

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 Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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 Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

By submitting a proposal, bidder certifies that no relationship exists between the bidder and any person or entity which either is, or gives the appearance of, a conflict of interest related to this Request for Proposal or project.

Bidder further certifies that bidder will not employ any individual known by bidder to have a conflict of interest nor shall bidder take any action or acquire any interest, either directly or indirectly, which will conflict in any manner or degree with the performance of its contractual obligations hereunder or which creates an actual or appearance of conflict of interest.

If there is an actual or perceived conflict of interest, bidder shall provide with its proposal a full disclosure of the facts describing such actual or perceived conflict of interest and a proposed mitigation plan for consideration. The State will then consider such disclosure and proposed mitigation plan and either approve or reject as part of the overall bid evaluation.

**J. ADVERTISING**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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 goods or 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.

**K. 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.

**L. DISASTER RECOVERY/BACK UP PLAN**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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 delivery of goods and services as specified under the specifications in the contract in the event of a disaster.

**M. DRUG POLICY**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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.

**N. WARRANTY**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			<b>We agree to comply and accept.</b>

Despite any clause to the contrary, the Contractor represents and warrants that its services hereunder shall be performed by competent personnel and shall be of professional quality consistent with generally accepted industry standards for the performance of such services and shall comply in all respects with the requirements of this Agreement. For any breach of this warranty, the Contractor shall, for a period of ninety (90) days from performance of the service, perform the services again, at no cost to the State, or if Contractor is unable to perform the services as warranted, Contractor shall reimburse the State all fees paid to Contractor for the unsatisfactory services. The rights and remedies of the parties under this warranty are in addition to any other rights and remedies of the parties provided by law or equity, including, without limitation actual damages, and, as applicable and awarded under the law, to a prevailing party, reasonable attorneys' fees and costs.

**O. LOBBYING**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			<b>We agree to comply and accept.</b>

1. No federal or state funds paid under this RFP shall be paid for any lobbying costs as set forth herein.
2. Lobbying Prohibited by 31 U.S.C. § 1352 and 45 CFR §§ 93 et seq, and Required Disclosures.



- a. Contractor certifies that no federal or state appropriated funds shall be paid, by or on behalf of Contractor, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this award for: (a) the awarding of any federal agreement; (b) the making of any federal grant; (c) the entering into of any cooperative agreement; and (d) the extension, continuation, renewal, amendment, or modification of any federal agreement, grant, loan, or cooperative agreement.
  - b. If any funds, other than federal appropriated funds, have been paid or will be paid to any person for influencing or attempting to influence: an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with Contractor, Contractor shall complete and submit Federal Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
3. Lobbying Activities Prohibited under Federal Appropriations Bills.
- a. No paid under this RFP shall be used, other than for normal and recognized executive-legislative relationships, for publicity or propaganda purposes, for the preparation, distribution, or use of any kit, pamphlet, booklet, publication, electronic communication, radio, television, or video presentation designed to support or defeat the enactment of legislation before the Congress or any State or local legislature or legislative body, except in presentation of the Congress or any State or local legislature itself, or designed to support or defeat any proposed or pending regulation, administrative action, or order issued by the executive branch of any state or local government itself.
  - b. No funds paid under this RFP shall be used to pay the salary or expenses of any grant or contract recipient, or agent acting for such recipient, related to any activity designed to influence the enactment of legislation, appropriations, regulation, administrative action, or Executive order proposed or pending before the Congress or any State government, State legislature or local legislature or legislative body, other than normal and recognized executive legislative relationships or participation by an agency or officer of an State, local or tribal government in policymaking and administrative processes within the executive branch of that government.
  - c. The prohibitions in the two sections immediately above shall include any activity to advocate or promote any proposed, pending or future federal, state or local tax increase, or any proposed, pending, or future requirement or restriction on any legal consumer product, including its sale of marketing, including but not limited to the advocacy or promotion of gun control.
4. Lobbying Costs Unallowable Under the Cost Principles. In addition to the above, no funds shall be paid for executive lobbying costs as set forth in 45 CFR § 75.450(b). If Contractor is a nonprofit organization or an Institute of Higher Education, other costs of lobbying are also unallowable as set forth in 45 CFR § 75.450(c).

**P. AMERICAN WITH DISABILITIES ACT**

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			<b>We agree to comply and accept.</b>

Contractor shall comply with all applicable provisions of the Americans with Disabilities Act of 1990 (42 U.S.C. 12131–12134), as amended by the ADA Amendments Act of 2008 (ADA Amendments Act) (Pub.L. 110–325, 122 Stat. 3553 (2008)), which prohibits discrimination on the basis of disability by public entities.

**IV. PAYMENT**

**A. PROHIBITION AGAINST ADVANCE PAYMENT (Statutory)**

Neb. Rev. Stat. §81-2403 states, “[n]o goods or services shall be deemed to be received by an agency until all such goods or services are completely delivered and finally accepted by the agency.”

**B. TAXES (Statutory)**

The State is not required to pay taxes and assumes no such liability as a result of this solicitation. The Contractor may request a copy of the Nebraska Department of Revenue, Nebraska Resale or Exempt Sale Certificate for Sales Tax Exemption, Form 13 for their records. 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 Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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

- Billing period
- Number of calls handled and/or made
- Average Handled Time (AHT)
- The tier you are billing for and the dollar amount
- Printing and postage dollar amount. On an attached document itemize the postage and printing with. Customer name, number of pages printed, postage amount and the mailing date.

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 Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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 corporate 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 (Statutory)**

Payment will be made by the responsible agency in compliance with the State of Nebraska Prompt Payment Act (See Neb. Rev. Stat. §81-2403). 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 goods and 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 (Statutory)**

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.

**H. RIGHT TO AUDIT (First Paragraph is Statutory)**

The State shall have the right to audit the Contractor's performance of this contract upon a thirty (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. (Neb. Rev. Stat. §84-304 et seq.) 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.

Accept (Initial)	Reject (Initial)	Reject & Provide Alternative within Solicitation Response (Initial)	NOTES/COMMENTS:
GR			We agree to comply and accept.

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 three (3) percent 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 (90) days of written notice of the claim. The Contractor agrees to correct any material weaknesses or condition found as a result of the audit.

## **V. PROJECT DESCRIPTION AND SCOPE OF WORK**

### **A. PROJECT OVERVIEW**

The State of Nebraska is issuing this Request for Proposal (RFP) to solicit proposals from qualified bidders to provide additional call center support services for ACCESSNebraska. The State of Nebraska requires additional customer service resources to answer inbound calls and/or perform customer outreach activities including providing back-office processing services. Bidder must submit proposals to provide all services.

The Department of Health and Human Services administers and manages eligibility for Medicaid and Economic Assistance programs through ACCESSNebraska. ACCESSNebraska provides a convenient way for Nebraskans to apply for the following Nebraska Medicaid and Economic Assistance programs:

- Medicaid
- Supplemental Nutrition Assistance Program (SNAP)
- Aid to Dependent Children (ADC)
- Aid to Aged, Blind and Disabled (AABD) Payment
- Low Income Home Energy Assistance Program (LIHEAP)
- State Disability Program
- Child Care Subsidy
- Refugee Resettlement Program
- Social Services for the Aged and Disabled (SSAD)

### **B. PROJECT ENVIRONMENT**

ACCESSNebraska provides services to obtain benefits through a number of methods:

- Five (5) Customer Service Centers (CSC) - Fremont, Lexington, Lincoln, Omaha and Scottsbluff.
- Currently augmented by two (2) contracted call centers, which assist by handling change requests, entering applications and responding to status calls.
- 54 (fifty-four) Local offices across Nebraska
- ACCESSNebraska Document Imaging Center in Omaha
- Web – ACCESSNebraska.ne.gov

Currently the CSCs:

- Receive between 51,000 (fifty-one thousand) – 68,000 (sixty-eight thousand) incoming calls a month.
- Receive 5,200 (five thousand two hundred) -6,700 (six thousand seven hundred) calls per day, on the peak days of the month.
- Peak day(s) are generally the first week of the month and the day after a holiday.
- The average length of a call is 12 (twelve) to 30 (thirty) minutes.

### **C. SCOPE OF WORK**

Contractor will receive inbound calls from individuals seeking ACCESSNebraska services; vendor will provide updates of the status of service requests processing and assistance in the completion of change requests and application(s). Bidders will provide per call costs, training per hour per person cost and the cost for start-up expenses. Printing and postage costs for mailings to individuals will be reimbursed monthly by DHHS with no additional markup. DHHS will supply pre-printed envelopes. Bidder will provide a cost for start-up expenses incurred prior to beginning to provide inbound call services.

Contractor will provide outreach services for individuals seeking ACCESSNebraska services; vendor will provide outbound calling and back-office processing services to assist in the completion of application(s). Outreach will include but not limited to tasks such as scheduling appointments for interviews and processing returned mail. Back-office processing is work the Contractor would be assigned to support some aspect of ACCESSNebraska. The work includes but not limited to tasks like data entry, data lookup, document indexing or document scanning. One example of back-office processing would be handling returned mail, looking up new addresses in online tools, and updating the address of record in the designated system. Assignment of this work will be done through the ACCESSNebraska web-based system, lists or other electronic means. Bidders will provide per outreach activity costs and the cost for start-up expenses. Printing and postage costs for any mailings will be reimbursed monthly by DHHS With

no additional markup. DHHS will supply pre-printed envelopes. Bidder will provide a cost for start-up expenses incurred prior to beginning to provide services. The call center and remote workers shall all be located within the United States.

## 1. BUSINESS REQUIREMENTS

- a. Answer inbound calls routed to them and conduct outreach calls on behalf of ACCESSNebraska from 8:00 AM through 6:00 PM Central time, Monday through Friday, with the exception of State holidays defined in state law.
- b. Provide an (800) number for routing of calls.
- c. Contractor must answer calls with a maximum Average Speed of Answer (ASA) of five (5) minutes.
- d. Contractor will enter information regarding the call as needed, either utilizing the ACCESSNebraska web application located at [www.accessnebraska.ne.gov](http://www.accessnebraska.ne.gov), DHHS N-FOCUS application, or other DHHS systems that may be made available.
- e. Information and data received or created by the Contractor in providing services under this contract will only be entered into the ACCESSNebraska.ne.gov website, the contractor's Customer Relationship Management system, or other systems that may be made available by DHHS. Contractor will ensure that no information and data gathered in providing services under this contract is entered, stored, or maintained elsewhere, except as necessary to perform the work. Additionally, such information and data will only be used for the purposes identified in this contract and is the property of DHHS.
- f. Contractor will store and process information and data received or created by Contractor in providing services under this contract in a secure manner such that unauthorized persons cannot gain access to it by means of a computer, remote terminal, or other means, and to ensure that only authorized persons will have access to such information and data.
- g. Contractor will provide and utilize a Customer Relationship Management (CRM) system to document the number and category of services provided. The information in this system shall be made available to DHHS upon request.
- h. Contractor must ensure all agents are supplied with telephony software, telephony equipment, computer equipment and software, and all network infrastructure to provide the service. The State will not provide any equipment.
- i. Contractor must adhere to all DHHS and Nebraska Information Technology Commission (NITC) security standards and policies. Links are found here: [https://dhhs.ne.gov/Documents/Information%20Technology%20\(IT\)%20Security%20Policies%20and%20Standards.pdf](https://dhhs.ne.gov/Documents/Information%20Technology%20(IT)%20Security%20Policies%20and%20Standards.pdf) and <https://nitc.nebraska.gov/standards/index.html>
- j. If the Contractor is utilizing telework, the Contractor must ensure that staff has the equipment necessary to perform the work effectively and efficiently, this may include but not be limited to a suitable laptop or other device, additional monitor(s) and a phone. Contractor will also ensure that the staff has a secure location to do business that will keep all client information confidential and safe.
- k. Contractor will support remote access technologies as defined by DHHS (virtual desktop infrastructure and multi-factor authentication).
- l. Contractor will follow all DHHS procedures provided through training, using a "Train the Trainer" method, initially during the contract startup of the contract and as needed for any new processes amended into the contract.
- m. The Contractor is responsible for all oversight and management of staff including hiring, training, onboarding, tracking time sheets and performing payroll.
- n. Contractor shall protect any Personal Health Information (PHI) and Personal Identifying Information (PII) in accordance with federal law, including 42 CFR Part 431 Subpart F, and Centers for Medicare and Medicaid Services (CMS) guidance using the National Institute of Standards and Technology (NIST 800-53) control framework. Adherence to the guidance shall be evaluated by a qualified independent third party at the Contractor's expense, evaluation includes annual security controls assessment and a penetration test.
- o. Contractor will provide DHHS view only access to Contractor's automatic call distribution (ACD) system to assist with call volume distribution.
- p. Contractor shall provide both English and Spanish language interpretation services. At all times during Business Hours, at least 10% (ten percent) of agents must be fluent in reading, writing, and speaking in Spanish and English. For non-English and non-Spanish language interpretation services, the Contractor must supply a method of telephonic interpretation. Cost of interpretation services shall be included in cost per call.
- q. Upon termination of this contract, Contractor shall transfer or return all information and data obtained in providing services under this contract to DHHS and/or delete such data upon DHHS

written request. The parties agree to negotiate in good faith, and mutually agree upon the format, timing, and manner for such transfer or return of information and data.

- r. Contractor must record all inbound and outbound calls.
  - i. Recorded calls shall be named in the following format: [automatic number identification (ANI)] [Call Type] [@] [HH\_MM AM (or PM)] [MM DD YY].
  - ii. Audio files of the recorded calls shall be sent to DHHS daily, via secure method approved by DHHS. Audio files shall be delivered to DHHS by 10:00AM on the next business day.
  - iii. Recorded calls shall be permanently deleted after successful transfer to DHHS.
  - iv. Call transfer validation process shall be established by the contractor with the review and approval by DHHS.
- s. Any data that is stored on site including multi-function devices, needs to be secured per DHHS policies. Links are found here:  
[https://dhhs.ne.gov/Documents/Information%20Technology%20\(IT\)%20Security%20Policies%20and%20Standards.pdf](https://dhhs.ne.gov/Documents/Information%20Technology%20(IT)%20Security%20Policies%20and%20Standards.pdf) and <https://nitc.nebraska.gov/standards/index.html>
- t. Mail customers a paper copy of the requested changes and/or applications, if applicable.
- u. Contractor must only print personal client information when necessary, and only in private office space that is distinctly separate from any publicly accessible area by a wall or other suitable barrier. Any door accessing this private office space shall be secured by a locking mechanism (key, number combination, access card, etc).
- v. Contractor will maintain Quality Assurance (QA) accuracy at or above an agreed upon level using an agreed upon evaluation tool. An established timeline to meet this performance measure will be included in Contractor Start-Up Plan. Attachment 5 - Sample Quality Assurance Form.
- w. Contractor will monitor at least five (5) calls from each agent per month. Quality scores for each agent will be made available for DHHS oversight staff.
- x. Contractor will utilize the DHHS approved quality evaluation tool to evaluate specific interactions between staff and clients.
  - i. Will meet with DHHS bi-weekly for calibration sessions.
  - ii. DHHS will select and send four (4) random contractor received calls to score at least 3 days prior to the calibration session.
  - iii. All participants will score each call-in advance using an agreed-upon evaluation form. Attachment 6 – Sample Quality Evaluation Scoring Report Template.
  - iv. Sessions will consist of introducing each call and then sharing evaluation scores to see how evaluations can be completed more consistently.
  - v. Notes will be taken by DHHS for general coaching notes for staff and any enhancement requests for training in these meetings.
  - vi. DHHS will conduct regular call evaluations and provide feedback to the contractor.
  - vii. All feedback will be logged by DHHS on a secured shared drive. Access to the secured shared drive will be provided to the contractor. DHHS will specify which evaluations require feedback from the contractor which will include documentation of action taken and the date.

## 2. REPORT REQUIREMENTS

Contractor must provide the following reports via email or file share:

- a. Daily report with number of offered and number of handled calls, Average Speed of Answer (ASA), Average Handled Time (AHT) by queue. See Attachment 7 – Daily Report Sample.
- b. Daily report the number of completed items by category:
  - i. Change Requests;
  - ii. Applications;
  - iii. Application status;
  - iv. Denial status inquiries from Contractor's CRM.
- c. Daily report for the outreach activities including:
  - i. Number of outreach activities per hour per agent;
  - ii. Average talk time per outreach;
  - iii. Most frequently asked questions/topics of concern;
  - iv. Most frequently used resources;
  - v. Number of outreach actions completed per hour/day/week;
  - vi. Number of voicemails left;
  - vii. Number of repeat callers.
- d. Ad hoc outreach statistic reports as requested. Due date for ad hoc call statistic reports will be determined by the Parties.
- e. Daily report with the quantity of calls or tasks completed for any other assigned work types
- f. Weekly report of QA monitoring metrics.

- g. Weekly QA Calibration reporting.
- h. Weekly summary reports shall be provided via email to the DHHS Contract Manager or designee, no later than 12:00 noon (Central Time) Tuesday of each week.
- i. Daily reports of the prior workday shall be provided via email no later than 9:30 am CST.
- j. Contractor shall provide ad hoc reports as requested by the State. Due date for ad hoc reports will be determined by mutual agreement of the parties.

**3. STATE RESPONSIBILITIES**

- a. Provide and maintain Contractor access to DHHS systems as required.
- b. Provide access to location where recorded calls will be stored.
- c. Make telephone line(s) available for Contractor's use.
- d. Route calls to the Contractor.
- e. Provide system testing to ensure call transfer operates properly.
- f. Provide Contractor with procedures for voice signature and other processes as needed.
- g. Provide written reference and consultative materials Contractor must use when answering questions from callers. The State will provide updates to reference and consultative materials as necessary.
- h. Provide training materials and train-the-trainer sessions, including but not limited to,

**ACCESSNebraska Base Curriculum (12 hours total)**

- i. Confidentiality -HIPAA
- ii. Eligibility Operations
- iii. Getting Started
- iv. Navigation Options
- v. N-FOCUS Help
- vi. Finding Persons in N-FOCUS
- vii. Person List Window
- viii. Search by SSN
- ix. Additional Person Search Options
- x. Performing Person Search Quiz
- xi. Master Case Search
- xii. Search by MC by Name
- xiii. Managed Care
- xiv. EBT Card
- xv. Authorized Representative
- xvi. Applications - The Basics
- xvii. Duplicate Application
- xviii. Phone Applications
- xix. Spanish Application
- xx. Viewing Applications
- xxi. Renewal/Recertification
- xxii. Document Imaging
- xxiii. Where can I find Correspondence?
- xxiv. Correspondence Examples
- xxv. Scheduled Interview
- xxvi. Assignments
- xxvii. Required Verifications
- xxviii. Verification Request
- xxix. Change Reports
- xxx. Programs
- xxxi. Eligibility Summary
- xxxii. Commonly Asked Questions
- xxxiii. Escalated Calls
- xxxiv. AccessNebraska Website Education

**VERIFICATION REQUEST FOLLOW UP TRAINING (3 hours total)**

- i. What is a Verification Request
- ii. Verification Request Follow Up Engagement
- iii. How to view a Verification Request
- iv. Verification Request is Open
- v. Partial Verification Request

**INTERVIEW FOLLOW UP TRAINING (1.5 hours total)**

- i. What is an interview
- ii. Interview Follow Up Engagement

- iii. Scheduled Interview
- iv. Interview Has Not Been Completed
- i. Provide access to Annual Security Awareness Training.
- j. Schedule weekly meetings with Contractor to review performance.
- k. See Attachment 8 – Monthly Call Volume for estimated monthly and daily call volumes to be answered by the contractor(s).
- l. Upon execution of the contract, DHHS will supply current half-hour call volumes to the contractor(s).
- m. Provide pre-printed DHHS mailing envelopes.

**4. PRICING STRUCTURE**

Because of the uncertain future extent of the need for additional ACCESSNebraska call center assistance in Nebraska, the State is requesting proposals to provide per call/action pricing for tiered levels of inbound call services, outreach services and back-office processing services per month according to the table below.

Service		Average Handled Time (AHT)	Number of calls/actions Tier I	Number of calls/actions Tier II	Number of calls/actions Tier III
<b>Inbound</b>	A	11:00-15:00	6,000-16,999	17,000-27,999	28,000-40,000
	B	15:01-20:00	1,400-3,599	3,600-5,799	5,800-8,000
	C	20:01-25:00	1,400-3,599	3,600-5,799	5,800-8,000
	D	25:01-30:00	1,400-3,599	3,600-5,799	5,800-8,000
	E	30:01-35:00	1,400-3,599	3,600-5,799	5,800-8,000
<b>Outreach</b>	A	8:00 -12:00	1,400-3,599	3,600-5,799	5,800-8,000
	B	12:01 - 16:00	1,400-3,599	3,600-5,799	5,800-8,000
	C	16:01 - 20:00	1,400-3,599	3,600-5,799	5,800-8,000
<b>Back Office Processing</b>	A	4:00-8:00	1,400-3,599	3,600-5,799	5,800-8,000
	B	8:01 - 12:00	1,400-3,599	3,600-5,799	5,800-8,000
	C	12:01-16:00	1,400-3,599	3,600-5,799	5,800-8,000

- a. Contractor must provide:
  - i. Training cost per hour per agent.
  - ii. Any Telecom costs for outbound calls must be included within tiered pricing structure.
  - iii. Any report costs must be included within tiered pricing structure.
  - iv. Printing at cost per page as defined by the bidder on Attachment 4 – Cost Proposal Sheet
  - v. Postage monthly expenses are reimbursed at cost by DHHS.
- b. If the State requires additional inbound call capacity, the State will notify Contractor, in writing, of the increased call capacity required. Contractor will provide additional inbound call capacity and begin training no later than three (3) weeks after receipt of request from the State.
- c. The State and Contract may negotiate pricing and capacity for any increase in volume over Tier III. Contractor may request up to thirty (30) days' notice for any such negotiated increase over Tier III call volume.

**5. DELIVERABLES**

The Contractor shall provide the following deliverables:

- a. Start-Up Plan, which includes a schedule, Gantt chart, and milestones for the first month of services. The Contractor's Start-Up Plan must contain the following items:
  - i. Program Implementation;
  - ii. Discovery Phase;
  - iii. Standard Operating Procedure (SOP) Process Mapping;
  - iv. SOP Read-out;



- v. Technology Set-up
  - vi. Custom CRM;
  - vii. ACD/IVR;
  - viii. Email Platform;
  - ix. Quality Assurance System;
  - x. Initial Training Development;
  - xi. Training for staff; and,
  - xii. Go-live date.
  - xiii. Third-party IT security attestation completion date and report.
- b. Training for contractor's call center staff as a pass-through cost.
  - c. Provide daily services and reports as specified in this RFP.
  - d. Per page printing at proposed pass-through cost.
  - e. Mailing reimbursement at cost.

## VI. PROPOSAL REQUIREMENTS

### PROPOSAL INSTRUCTIONS

This section documents the requirements that should be met by bidders in preparing the Solution and Cost Proposal. Bidders should identify the subdivisions of "Project Description and Scope of Work" clearly in their proposals; failure to do so may result in disqualification. Failure to respond to a specific requirement may be the basis for elimination from consideration during the State's comparative evaluation.

Proposals are due by the date and time shown in the Schedule of Events. Content requirements for the Solution and Cost Proposal are presented separately in the following subdivisions; format and order:

#### A. PROPOSAL SUBMISSION

##### 1. CORPORATE OVERVIEW

The Corporate Overview section of the Solution Proposal should consist of the following subdivisions:

###### a. CONTRACTOR 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 first organized to do business and whether the name and form of organization has changed since first organized.

###### b. 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.

###### c. CHANGE OF 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 bidder(s) will require notification to the State.

###### d. OFFICE LOCATION

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

###### e. RELATIONSHIPS WITH THE STATE

The bidder should describe any dealings with the State over the previous five (5) 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.

###### f. 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 twelve (12) 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.

g. **CONTRACT PERFORMANCE**

If the bidder or any proposed Subcontractor has had a contract terminated for default during the past five (5) 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 contractor submit full details of all termination for default experienced during the past five (5) 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 five (5) years, so declare.

If at any time during the past five (5) 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.

h. **SUMMARY OF BIDDER'S CORPORATE EXPERIENCE**

The bidder should provide a summary matrix listing the bidder's previous projects similar to this solicitation 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 contractor's experience and this solicitation. These descriptions should include:
  - a) The time period of the project;
  - b) The scheduled and actual completion dates;
  - c) The bidder'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 contractor 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. Bidder 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 bidders above. In addition, Subcontractors should identify what share of contract costs, project responsibilities, and time period were performed as a Subcontractor.

i. **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 solicitation. 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 solicitation 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.

j. **SUBCONTRACTORS**

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

- iv. name, address, and telephone number of the Subcontractor(s);
- v. specific tasks for each Subcontractor(s);
- vi. percentage of performance hours intended for each Subcontract; and
- vii. total percentage of Subcontractor(s) performance hours.

**2. SOLUTION APPROACH**

The solution approach section of the Proposal should consist of the following subsections:

- 1. Understanding of the project requirements;
- 2. Proposed development approach;
- 3. Technical considerations;
- 4. Detailed project work plan; and
- 5. Deliverables and due dates.

**3. REQUIRED BIDDER RESPONSES**

Attachment 3 - Required Bidder Responses

**4. COST PROPOSAL**

Attachment 4 – Cost Proposal Sheet

**VII. ATTACHMENTS**

- 1. Attachment 1 – Form A - Bidder Proposal Point of Contact
- 2. Attachment 2 – Form B - Request for Proposal for Contractual Services Form
- 3. Attachment 3 – Required Bidder Responses
- 4. Attachment 4 – Cost Proposal Sheet
- 5. Attachment 5 – Sample Quality Assurance Form
- 6. Attachment 6 – Sample Quality Evaluation Scoring Report Template
- 7. Attachment 7 – Daily Report Sample
- 8. Attachment 8 – Monthly Call Volume

# ATTACHMENT 1

## Form A Bidder Proposal Point of Contact Request for Proposal Number 113578 O3

Form A should be completed and submitted with each response to this solicitation. 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:	Conversion Calls LLC
Bidder Address:	1830 N University Dr. Suite 385 Plantation, FL 33322
Contact Person & Title:	Matthew Hanusa
E-mail Address:	mhanusa@conversioncalls.com
Telephone Number (Office):	954.234.2575
Telephone Number (Cellular):	913.209.2502
Fax Number:	

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:	Conversion Calls LLC
Bidder Address:	1830 N University Dr. Suite 385 Plantation, FL 33322
Contact Person & Title:	Matthew Hanusa
E-mail Address:	mhanusa@conversioncalls.com
Telephone Number (Office):	954.234.2575
Telephone Number (Cellular):	913.209.2502
Fax Number:	

ATTACHMENT 2

FORM B

REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM

**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 Solicitation, and agrees to the terms and conditions unless otherwise indicated in writing and certifies that bidder maintains a drug free work place.

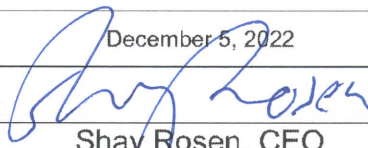
Per Nebraska's Transparency in Government Procurement Act, Neb. Rev Stat § 73-603 DAS is required to collect statistical information regarding the number of contracts awarded to Nebraska Contractors. This information is for statistical purposes only and will not be considered for contract award purposes.

\_\_\_\_\_ 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 Solicitation.

\_\_\_\_\_ 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 MANUALLY IN INK OR BY DOCUSIGN**

FIRM:	Conversion Calls LLC
COMPLETE ADDRESS:	1830 N University Dr. Suite 385 Plantation, FL 33322
TELEPHONE NUMBER:	954 607 2019
FAX NUMBER:	
DATE:	December 5, 2022
SIGNATURE:	
TYPED NAME & TITLE OF SIGNER:	Shay Rosen, CEO



**State of Nebraska  
Department of Health & Human Services**

**RFP# 113578 O3  
Additional Call Center Support Services  
for ACCESSNebraska**

*Response Submitted By:*

**Conversion Calls LLC**  
Matthew Hanusa, SVP  
1830 N. University Drive, Ste 385  
Plantation, FL 33322  
(o) 954-234-2575  
(m) 913-209-2502

**NEBRASKA**

Good Life. Great Mission.

---

**DEPT. OF HEALTH AND HUMAN SERVICES**



**December 5, 2022**

**Subject: Conversion Calls response to RFP# 113578 O3**

Dear State of Nebraska and the Department of Health & Human Services:

Conversion Calls is pleased to submit our proposal response for the requested additional call center support services for ACCESSNebraska. Incorporated in 2006, Conversion Calls is a diverse small to medium sized business that was founded by immigrants who relocated to the United States, became citizens, and have more than 16 years of experience providing unique solutions to Public / Government Agencies and Public Institutes of Higher Education. We are currently providing similar call center and customer support services for the Colorado Department of Labor & Employment (CDLE), in which we service and support up to 300,000 customers during peak times. Our initial contract with them was about 1.5 years and last Fall (November 2021) they extended with us another five years based upon our world-class customer service, operational excellence, and flexibility and customization toward their organization and citizen's needs.

With over 16 years of experience providing similar services, Conversion Calls has a diverse experience and skill set that matches your requirements closely. **We acknowledge you have current partners and are looking to expand for additional support. We ask that as a public state agency, we are granted a full and fair review and that you transition to and/or expand with Conversion Calls because our success lies in our understanding and experience of the current operation and its needs, proactively analyzing the data, providing world-class customer service, and providing a customized solution that will best suits your needs for a seamless transition with differentiators such as:**



- **The senior executive leader (Matthew Hanusa) that we are assigning to this project initiative was raised, grew up, and spent over 30+ years in Nebraska. He understands the culture of the state, the urban, suburban, and rural communities, the needs of your citizens, and will build rapport quickly with all of you as a peer, a strategic partner, and a Nebraskan as he will ensure that you and your resident's needs are fully supported and met / exceeded.**
- **Our focus and specialty is the Public Sector, which includes state agencies, public higher ed, etc.**
- **Week-to-Week Up or Down Agent Scalability (vs 30 days-notice which is typical).**
- **We have the resources to have up to 150 agents ready for training every seven days and its mandatory they are US based.**
- **We are glad to transition any incumbent team members (as appropriate) to our team and/or assign Nebraska residents to the dedicated agent team to promote a seamless transition.**
- **We are available 24/7, and therefore have no challenges covering your hours of operation and extended hours or holidays if needed.**
- **We offer a seven-day notice on any contract changes or opt outs if that resonates with you as a benefit.**
- **Proactive access, knowledge, and experience of best practices from other state entities.**
- **We are not just a staffing agency as we provide the agents, the managers, the supervisors, the training, the quality assurance, the data security and compliance, and the required technology & support they need to do the job successfully.**
- **We are fully compliant when it comes to PII, Information and Data security, HIPAA, HECVAT, etc.**



*We take every call personally*

- **We can and will provide the training as we offer a train the trainer model to save you time and resources, and our IT and telephony team are experts at IVR programming and best practices if you would like us to proactively partner with your team.**

Conversion Calls will perform the contract within the specified time frames as well as provide you with a day-one service. Our goal is minimizing any disruption of the current operation while implementing our solution.

We have significant experience transitioning and/or integrating with large public organizations and look forward to working with your team. We have the experience, capability, and capacity to successfully implement and deliver the needs of this RFP.

The leadership team has reviewed the RFP and all subsequent amendments and attachments in full detail, and we certify that our offering fully meets and/or exceeds all requirements of the RFP. We agree to the terms and conditions stated in the RFP documents. Conversion Calls certifies that all information presented in this proposal is accurate and should you need any clarification regarding this proposal submission, please contact me directly as I am available at your convenience to answer any questions that may arise during the proposal evaluation period.

Respectfully,

*Matthew Hanusa*

Matthew Hanusa, Senior Vice President  
(o) 954-234-2575  
(m) 913-209-2502  
mhanusa@conversioncalls.com

**TABLE OF CONTENTS**

**Corporate Overview ----- 5**

**Solution Approach ----- 12**

**Required Bidder Responses ----- attached separately**

**Cost Proposal ----- 26 and attached separately**

## **CORPORATE OVERVIEW**

### **Contractor Identification and Information**

#### **Conversion Calls LLC**

1830 N. University Drive, Ste 385  
Plantation, FL 33322

- Incorporated in Delaware
- Headquartered in Florida
- Founded in April 2006

### **Financial Statements**

- Please reference separately attached Financial Attestation.

### **Change of Ownership**

- None – Not Applicable

### **Office Location**

- As noted, Conversion Calls is headquartered in Florida.

### **Relationships with the State**

- Conversion Calls has no known relationships with the State of Nebraska and no prior state contracts. We have nothing to declare in this section.

### **Bidder's Employee Relations to the State**

- Conversion Calls has nothing to declare in this section as no such relationship exists, or has existed in any way or form.

### **Contract Performance**

- NA – Not Applicable as we have had no contracts terminated for the reasons mentioned in this section of the RFP. No issues with non-performance, no litigation, no issues with funding, etc.



*We take every call personally*

## **Summary of Bidder's Corporate Experience**

### **Experience 1 (Primary Contractor):**

Colorado Department of Labor & Employment (CDLE)  
Jeff Saeger  
L & EV CSC  
(303) 318-9428  
[jeff.saeger@state.co.us](mailto:jeff.saeger@state.co.us)

04/20 – present

Success = Five-year contract renewal in November 2021

Call Center Services for Unemployment Insurance Division

Conversion Calls role is providing a scalable extension inbound contact center agent team with some outbound, telephony, IVR, tech / tech support, quality assurance, etc since April 2020 to present. This project experience is relevant because over the past 2 years 8 months, we have provided them exactly what they needed in regarding to agent support on a weekly basis which has ranged from 100 to 650+ agents at any given time. In addition, our team performs similar services that you are asking for in this RFP and therefore we have the knowledge and experience you are looking for on top of being able to transition into other duties and tasks as well, apply best practices and more. For example, in addition to UI, PUA, etc, we assist with fraud prevention, call campaigns, state benefits, and new system program roll outs. Finally, after being partners with CDLE for 1.5 years, they extended with us for another 5 years which is a testimony to our track record, world class customer service, flexibility and customization in understanding the needs of their organization and their citizens.

### **Experience 2 (Primary Contractor):**

Northern Kentucky University  
Britta Gibson  
Associate Director  
(859) 572-7625  
[gibsonb9@nku.edu](mailto:gibsonb9@nku.edu)

March 2020 – present

Success = We have a positive impact on customer contact rate with students and parents, conversion rate, application rate, and enrollment rate to meet and exceed their expectations for multiple years.

Contact center service for new students, applicants, and requests for information.



*We take every call personally*

The role we have is to conduct inbound and outbound calls to various students, qualify them and assess their need in the enrollment and application process, then transfer them to the university admissions team or the correct department to meet their needs, which includes student and family services.

NKU is a public / government sector university with almost 20,000 students. We provide them with a contact center service handling several thousands of calls per week that is very similar to the needs of serving state's citizens in that we assess the need, review applications, statuses, and more, verify PII, resolve the situation on our own or transfer to the correct department. FERPA compliance is very similar to HIPAA.

### **Experience 3 (Primary Contractor):**

Bellevue University  
Charles Wright  
Sr. Director  
(402) 557-7048  
[cwright@bellevue.edu](mailto:cwright@bellevue.edu)

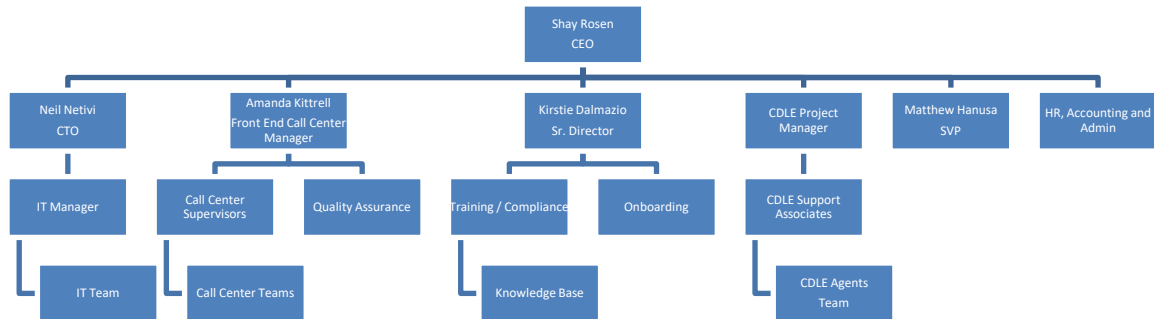
February 2020 - present

Success = Bellevue's student enrollment services continue to increase and this past Spring term their contact, conversion, and student results were 65% above prior year and this Fall was 25% over PY as we continue to have a positive impact year after year. This equates to more students and families receiving the services and benefits they need as we are accessing and communicating with more customers.

Contact Center service for inbound/outbound new student support, new applicant program support, new student inquiries, student success follow up, working adult / career partnership services, etc.

Our role is to provide a contact center team that handles all the services above for a private university **in Nebraska** with about 20,000 students and handling close to 75,000 calls per month. It is relevant because the needs of students and families is very similar to the needs and services provided by the State. For example, application support services, addressing basic questions and resolving, verifying PII, receiving calls and making outbound campaign communications, FERPA compliance is very similar to HIPAA, and more.

**Summary of Bidder’s Proposed Personnel / Management Approach**



**Client-Focused Customer Service:**

Conversion Calls strives to not only meet but exceed all customer service benchmarks and expectations. As our client-partner, your organization will be a top priority as we are flexible and customizable in all we do. Starting with the personal attention of senior leaders, your team will have a direct link to the Conversion Calls executive team and CEO keeping the lines of communication open and available at all times which means there is no red tape and minimal wait time as decisions and adjustments can be made almost instantly as we will pivot with you quickly. Our leadership and key personnel have extensive experience in call center and customer support solutions, the public and government sector, and public higher ed, etc. We have provided resume bios of key personnel assigned to this partnership below and will expand our superior support as needed to ensure strong outcomes and peace of mind:

**Shay Rosen, CEO (Time: As much as needed & available 24/7)**

- *Over 25 years of international business experience, specializing in call center and customer service management, sales, and digital marketing.*
- *In 2006 co-founded Conversion Calls with the purpose of catering to higher education and the public sector in all areas of contact center, customer service, answering services, application processing, verification and qualification services, and other service and marketing aspects.*
- *In the past 16 years, hands on led Conversion Calls and was able to position it as one of the premier companies in the sector, expanded into the public / government sector and proudly maintains long lasting remarkably successful partnerships with multiple public colleges and universities across the country.*

**Neil Netivi, CTO (Time: As much as needed & available 24/7)**

- *Over 25 years of IT, programming, and technology experience.*
- *Holds multiple degrees (master's level) and certifications in IT and network security.*
- *In 2006 co-founded Conversion Calls with the purpose of catering to higher education and the public sector in all areas of contact center, customer service, answering services, application processing, verification and qualification services, and other service and marketing aspects.*
- *At Conversion Calls, while managing a team of talented programmers and IT experts, was able to develop a line of proprietary systems that allows Conversion Calls to provide superior services to its partner clients. Among those services are high level integrations with cloud-based telephony, IVR expertise, integration with client CRM systems and internal reporting, recording, and monitoring systems.*



**Kirstie Boyle - Senior Director (Time: 100%)**

- *Kirstie joined Conversion Calls six years ago and came to us with over 25 years of professional experience in sales, marketing, operational excellence, training, and leadership. As Senior Director, she was and is charged with building out the contact center and customer support services along with training, updating the knowledge base, etc. Under her leadership, teams and procedures specific to each client-partner have been developed as the teams truly act as an extension of each organization and/or department.*
- *Kirstie has a strong ability to adapt and pivot as needed and is highly skilled at integrating into organizations. She prides herself on these outcomes and developing highly professional teams that are all-in for our strategic partners and their clients and customers.*

**Amanda Kittrell – Manager, Contact Center (Time: 100%)**

- *4 years-experience combined as an agent, effectively scheduling and supervising, and managing contact center team members and operations in onsite and remote work environments while managing quality assurance, observations, feedback, and coaching in partnership with the Senior Director and other assigned supervisors that will be assigned to lead this agent team for this project.*

**Matthew Hanusa, MBA - Senior Vice President (Time: As much as needed, available 24/7, and can office out of Nebraska as needed)**

- *25+ years of overall professional career experience.*
- *16+ years of agent, trainer, director level, and senior executive leadership experience (11 years) in contact center implementations and other operations and leadership roles.*

- *EXECUTIVE LEADER – operations, strategic planning, mission critical initiatives, innovation, customer-centric focus, fiscal accountability, dynamic team building, organizational effectiveness, and change management.*
- *CONTACT CENTER MANAGEMENT – private, non-profit, and public organizations, establishing efficiencies, metrics/benchmarks, conversions, forecasting, strategic call-center initiatives, business intelligence and systems expertise, and multi-site/state management.*

Applicable Contact Center Experience / Title in addition to experience above:

- **Conversion Calls - Senior Vice President: July 2019 – Present, 3.5 years**  
*\*Contact Center service solution provider, project manager, and client manager. Has helped many clients launch new contact center initiatives with complete success. Public Agencies supported to date: **Colorado Department of Labor & Employment, University of Maryland / UMGC, Colorado State University / CSU Global, Northern Vermont University, Northern Kentucky University, University of Idaho, College of DuPage, & Richard Bland Community College.***
- **Northeastern University – Associate Vice President: 2 years**  
*\*Tasked, and with 100% success built out and launched a new enrollment management contact center and team that supported online and adult domestic and international students for the Lifelong Learning Division, College of Professional Studies, the Regional Campuses, and extension programs from the traditional colleges throughout the entire admissions and enrollment process all the way through to term start. Included new applicants, program eligibility, transcript review, financial aid & scholarships, registrar, FERPA compliance, student services, advising, and more.*
- **Colorado Christian University – Vice President: 2 years**  
*\*During this time of rapid enrollment growth of 40% over PY, tasked with and successfully launched a new contact center telephony system, implemented an enrollment compliance and training department, and expanded the online contact center enrollment team by almost 100%. Included new applicants, program eligibility, transcript review, financial aid & scholarships, registrar, FERPA compliance, student services, advising, and more.*
- **Qwest Communications / AT&T – Contact Center Agent, Manager, and Trainer & Project Manager: 5 years**

### **Subcontractors**

- Conversion Calls does not intend to use subcontractors.

## **SOLUTION APPROACH**

### **Understanding the Project Requirements & Proposed Development Approach**

Conversion Calls has thoroughly reviewed the business and reporting requirements on pages 30 and 31 of the primary RFP document and we fully understand and comply to meet and exceed the needs of the State of Nebraska, DHHS, ACCESSNebraska, and the citizens of Nebraska which includes programs such as Medicaid, SNAP, ADC, AABD, LIHEAP, State Disability, Child Care Subsidy, Refugee Resettlement Programs, and SSAD. All of our agents and team members are US Based as required and our approach of how we will accomplish the business and reporting requirements is as follows:

#### **Delivery-Focused Public Sector Approach**

We differentiate ourselves from the competition in our delivery-focused approach instead of the typical sales-focused approach. Our leadership and managers are highly experienced with public / government organizations and contact center management as we have provided these services for over 16 years. We are committed and responsible individuals who have a service-oriented approach and put our client's interests ahead of our own as compared to other firms with sales-oriented Account Managers as their primary contact.



Conversion Calls will assign a team specifically tasked with supporting your system, **your primary contact will be a senior leader that was raised, grew up and lived a few decades in Nebraska**, knows the area, knows the various communities, understands the cultures and the needs of citizens, and more. In addition, you will always have direct access to the CEO of Conversion Calls as we are available 24/7 and have a no red-tape policy (ie: we work quickly and will pivot quickly with you).

### **Process-Driven Organization**

Through our experience supporting large and diverse public government clients, Conversion Calls has honed our programs and processes to provide superior delivery and performance to our clients. Our mature operating protocol and processes are the cornerstone of our delivery model ensuring consistent delivery and quality across all verticals and geographies. We are confident in our abilities, and we will develop mutually beneficial metrics so that we deliver the same quality of service to the State of Nebraska – DHHS / ACCESSNebraska.

### **Seamless Incumbent Transition**

If needed and as appropriate, Conversion Calls understands that transitioning to or adding a new strategic partner demands a large effort, which in the beginning may require team members to operate differently than they did in the past. During this time, we need to keep stakeholders educated, motivated, and excited about the benefits we offer in both the short and long term. In order to accomplish this, Conversion Calls will partner with DHHS / ACCESSNebraska to develop a successful service solution that communicates and trains the team members efficiently and effectively.

### **Proven Customized Recruiting and Screening**

Conversion Calls has internal team members, bilingual operators, and maintains a pipeline of background checked candidates representing the required knowledge and skill set for this specific service that are all US Based (which is already a mandatory requirement at Conversion Calls). This pipeline planning greatly reduces our time to ensure the right team members by streamlining the process for our clients. In addition, we are glad to utilize willing incumbent team members as well and/or **assign or hire Nebraska residents too!**

### **Public Government Sector Solution Provider**

Our specific industry focus has given Conversion Calls the experience that allows us to quickly adapt to the state's needs, requirements, and preferences while also allowing us to invest in the right resources.

DHHS / ACCESSNebraska can also leverage Conversion Calls' expertise in public sector contact center management to design, develop and manage strategies and effectively control the costs. In addition, several of our team members are bilingual and will be assigned accordingly, and our telephony and IT team of Five9 experts are extremely talented at call center and system integration and set up, programming IVRs, we utilize preferred numbers for all of our clients, provide full inbound and outbound call center agent customer service, provide all necessary equipment to be successful, provide call verification and qualification every day for all clients, provide all reporting, training, & quality assurance, call recording and archiving for up to seven years, texting is available through our Five9 system, and data pass-backs.



All Service Requirements of inbound and outbound call coverage, email, etc, will be implemented with success and all staffing levels, on-call scheduling and rapid scalability on a week-to-week basis (vs monthly), schedules, and additional services will be maintained to achieve and exceed all service expectations highlighted in the RFP. Yes, we grant our client partners peace of mind with scalability up or down with 7 days-notice as compared to typical 30 days-notice, which allows the organization to pivot quickly to meet all call volumes throughout the year.

### **Client-Focused Customer Service**

Above all, Conversion Calls strives to not only meet, but exceed all customer service needs. As our business partner, you will be our top priority as we are **flexible and customizable** in all we do within and outside of the scope. In other words, we will not nickel and dime you for customization requests or work done outside of the standard scope as most vendor-partners will do. For example, we just completed a three-week customization reporting request for a client in Nebraska at no additional charge. They were very appreciative of the “cost” and were ecstatic with the outcome.

Starting with the personal attention of a senior leader, you will have a direct link to the Conversion Calls executive team and CEO keeping the lines of communication open and available at all times which means there is no red tape and minimal wait time as decisions and adjustments can be made almost instantly as we work on the fly and pivot quickly with all of our client partners.

### **Technical Considerations**

Conversion Calls fully responded to all questions within Attachment 3 and we have included many documents with hundreds of pages that review our technical capabilities, compliances in regard to PII, data and information security, HIPAA, and more not only for the agents and calls, but for the printing and mailing of private documents as well. We will meet and exceed your expectations in these areas, along with all reporting and our Quality Assurance as we are flexible and customizable and can utilize, match, or exceed the reporting and quality assurance forms provided as examples as part of the RFP. In addition, all calls will be handled by a live agent that is US Based, all coverage hours will be met, all answer times, handle times, and wait times will be within expectations or better, and we will scale up or down with 7 days-notice at any time to meet call volume expectations throughout the annual cycle (which is a tremendous advantage as most offer this on a 30 day-notice basis).

Conversion Calls is committed to conducting business in conformity with the regulations and standards that apply to the client-partnership. We stay compliant to these regulations and others referenced as applicable by:

1. Identifying authoritative documents that are applicable and retain.
2. Interpret and rationalize the requirements and assess within the spectrum the actual level that applies to us.
3. Manage the requirements through documentation, training, examination, and take action as needed.
4. Operate in transparency and adhere to expectations.

Compliance, confidentiality, and security are of utmost importance to Conversion Calls. Data and information security and technical support and management are very hands-on and available immediately for our team.



*We take every call personally*

Finally, we are proud to communicate that we have been assessed and pass the HECVAT standards for Public Institution / Organizations, which includes data and information security and PII standards, FERPA, HIPAA, etc. In addition, we have client partners that run internal monthly certifications and/or audits and we pass those as well each time. To date, there have not been any clients for which we have failed to meet their expectations in these areas as needed.

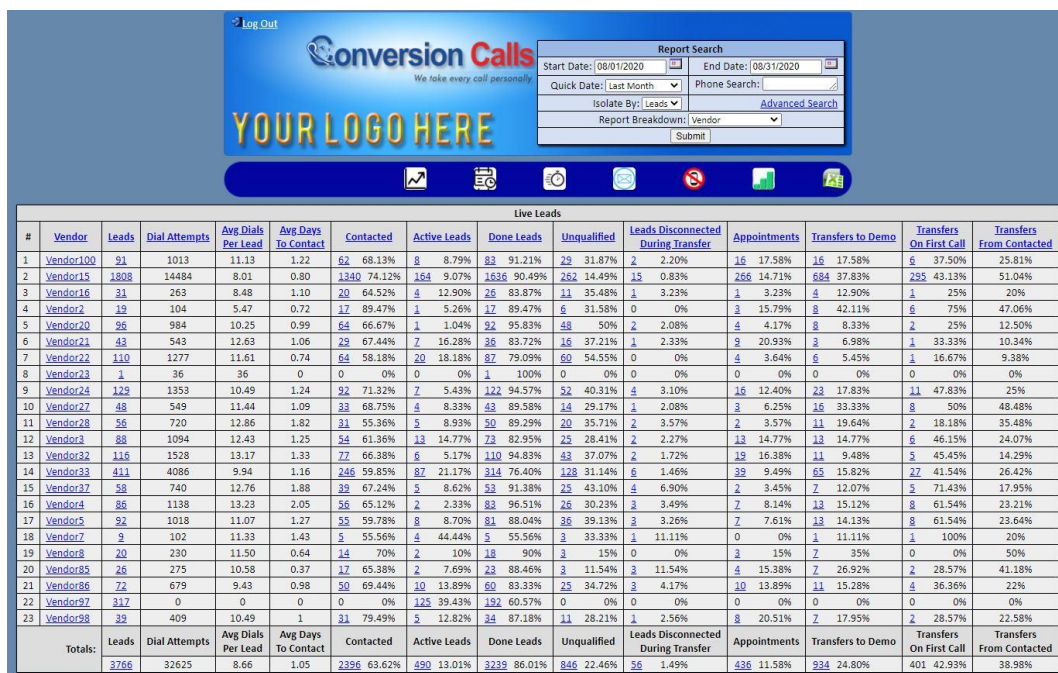
In summary, and as we all know, providing call center and customer service support for state agencies can include handling DOBs, social security numbers, tax returns, salary information, and address information. We have the capabilities and policies in place to be compliant in all areas that you expect us to be. As referenced and for your peace of mind, we have attached our “Conversion Calls Data Privacy Policy” along with other data security documents, disaster recovery and more. Please note, we have met all standards in this area for our current public entity clients. We will provide more information or updates upon request.

All metrics highlighted in the RFP will be captured along with any other metrics that DHHS requests. This can be done in real-time, daily, weekly, and can be sent to you manually via email, via secure file transfer, or we have a 24/7 online data portal that DHHS / ACCESSNebraska team members can access and view or download the data. We provide this at no additional cost and we are glad to provide a demo. Conversion Calls has reviewed the reporting and quality assurance list and we will provide all of this data and reporting in your format on a weekly, monthly, and quarterly basis (including graphs and spreadsheets). Our reporting capabilities are accurate, innovative, and will meet and exceed your expectations at all time. In addition, we can customize any other data reporting you’d like to view at any time.



### Valuable Online Data Reporting & Quality Assurance

Full Transparency: DHHS / ACCESSNebraska does not have to be concerned with scaling staffing, productivity, distracted or ill team members as all data is - Updated daily, and can be viewed by day, weekly, monthly, quarterly, or customized date ranges. In addition, all data can be exported to create additional reporting in excel, etc.



Live Leads																						
#	Vendor	Leads	Dial Attempts	Avg Dials Per Lead	Avg Days To Contact	Contacted	Active Leads	Done Leads	Unqualified	Leads Disconnected During Transfer	Appointments	Transfers to Demo	Transfers On First Call	Transfers From Contacted								
1	Vendor100	91	1013	11.13	1.22	62	68.13%	8	8.79%	83	91.21%	29	31.87%	2	2.20%	16	17.58%	16	17.58%	6	37.50%	25.81%
2	Vendor13	1808	14484	8.01	0.80	1340	74.12%	164	9.07%	1636	90.49%	262	14.49%	15	0.83%	266	14.71%	684	37.83%	295	43.33%	51.04%
3	Vendor16	31	263	8.48	1.10	20	64.52%	4	12.90%	26	83.87%	11	35.48%	1	3.23%	1	3.23%	4	12.90%	1	25%	20%
4	Vendor2	19	104	5.47	0.72	17	89.47%	1	5.26%	17	89.47%	6	31.58%	0	0%	3	15.79%	8	42.11%	6	75%	47.06%
5	Vendor20	96	984	10.25	0.99	64	66.67%	1	1.04%	92	95.83%	48	50%	2	2.08%	4	4.17%	8	8.33%	2	25%	12.50%
6	Vendor21	43	543	12.63	1.06	29	67.44%	7	16.28%	36	83.72%	16	37.21%	1	2.33%	9	20.93%	3	6.98%	1	33.33%	10.34%
7	Vendor22	110	1277	11.61	0.74	64	58.18%	20	18.18%	87	79.09%	60	54.55%	0	0%	4	3.64%	6	5.45%	1	16.67%	9.38%
8	Vendor23	1	36	36	0	0	0%	0	0%	1	100%	0	0%	0	0%	0	0%	0	0%	0	0%	0%
9	Vendor24	129	1353	10.49	1.24	92	71.32%	7	5.43%	122	94.57%	52	40.31%	4	3.10%	16	12.40%	23	17.83%	11	47.83%	25%
10	Vendor27	48	549	11.44	1.09	33	68.75%	4	8.33%	43	89.58%	14	29.17%	1	2.08%	3	6.25%	16	33.33%	8	50%	48.48%
11	Vendor28	56	720	12.86	1.82	31	55.36%	5	8.93%	50	89.29%	20	35.71%	2	3.57%	2	3.57%	11	19.64%	2	18.18%	35.48%
12	Vendor3	88	1094	12.43	1.25	54	61.36%	13	14.77%	73	82.95%	25	28.41%	2	2.27%	13	14.77%	13	14.77%	6	46.15%	24.07%
13	Vendor32	116	1528	13.17	1.33	77	66.38%	6	5.17%	110	94.83%	43	37.07%	2	1.72%	19	16.38%	11	9.48%	5	45.45%	14.29%
14	Vendor33	411	4086	9.94	1.16	246	59.85%	87	21.17%	314	76.40%	128	31.14%	6	1.46%	38	9.49%	65	15.82%	27	41.54%	26.42%
15	Vendor37	58	740	12.76	1.88	39	67.24%	5	8.62%	53	91.38%	25	43.10%	4	6.90%	2	3.45%	7	12.07%	5	71.43%	17.95%
16	Vendor4	86	1138	13.23	2.05	56	65.12%	2	2.33%	83	96.51%	26	30.23%	3	3.49%	7	8.14%	13	15.12%	8	61.54%	23.21%
17	Vendor5	92	1018	11.07	1.27	55	59.78%	8	8.70%	81	88.04%	36	39.13%	3	3.26%	7	7.61%	13	14.13%	8	61.54%	23.64%
18	Vendor7	9	102	11.33	1.43	5	55.56%	4	44.44%	5	55.56%	3	33.33%	1	11.11%	0	0%	1	11.11%	1	100%	20%
19	Vendor8	20	230	11.50	0.64	14	70%	2	10%	18	90%	3	15%	0	0%	3	15%	7	35%	0	0%	50%
20	Vendor85	26	275	10.58	0.37	17	65.38%	2	7.69%	23	88.46%	3	11.54%	3	11.54%	4	15.38%	7	26.92%	2	28.57%	41.18%
21	Vendor86	72	679	9.43	0.98	50	69.44%	10	13.89%	60	83.33%	25	34.72%	3	4.17%	10	13.89%	11	15.28%	4	36.36%	22%
22	Vendor97	317	0	0	0	0	0%	125	39.43%	192	60.57%	0	0%	0	0%	0	0%	0	0%	0	0%	0%
23	Vendor98	39	409	10.49	1	31	79.49%	5	12.82%	34	87.18%	11	28.21%	1	2.56%	8	20.51%	7	17.95%	2	28.57%	22.58%
Totals:		3766	32625	8.66	1.05	2396	63.62%	490	13.01%	3239	86.01%	846	22.46%	56	1.49%	436	11.58%	934	24.80%	401	42.93%	38.98%

1. We have 100% call recording and all recorded calls are available in our data portal 24/7 for DHHS / ACCESSNebraska to access anytime via search parameters.
2. Hourly tracking of contact, call, and transfer volume available each day for future analysis and adjustments to ensure the best customer service.



3. By analyzing the data and the outcomes of all calls and conversations, enhanced strategic decision-making can be made to continue to positively impact conversions and enrollment.
4. Access to recordings, dispositions, and more, are all available directly within the online portal.
5. Unique User ID and Password is given to primary client contact to distribute as appropriate, and the online portal is accessible 24/7.
6. We will comply with your data reporting sample and have provided customized examples attached separately. Once again, these were customized to meet client's needs.

As noted, Conversion Calls **will** comply and meet and/or exceed your quality assurance documents and expectations as requested. We want to demonstrate and communicate that our **Quality Assurance** management process and system is leveraged routinely to ensure compliance, employee effectiveness, professional demeanor at all times, training, and accountability to success. The goal is to observe at least 25% of the calls on average on a weekly and monthly basis, and our Quality Assurance System and documentation is all electronic and dynamic per the type of call it is.

**Quality Assurance Form Example – Call**

#	Agent Name	First Name	Last Name	Phone Number	Recording DateTime	Disposition	Duration	Download
1	KiaraLivingston	Adrean	Leflore	2489912340	9/1/2020 9:57:07 AM	I scheduled a call back time	00:52	<a href="#">Download</a>
Questions		Answers			Comments			
Did the agent start the conversation correctly ?		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Did the agent explain the purpose of the call ?		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Did the agent try to avoid setting a callback?		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Did the agent confirm the time zone? Eastern		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Did the agent mark correctly the reason for the call back? Busy		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Did the agent set the call back correctly? 9/04/2020 12:00:00 PM		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Disposition should be:		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	I scheduled a call back time			
General Comments:								
<a href="#">Submit</a>								

- 100% of all calls are recorded, saved for up to seven years, and fully accessible to the college team at any time 24/7.
- Attributes we observe, score, and hold team members accountable are:
  - A. Proper Greeting, Identifies Self, Verifies Student Info, Follows Scripting, and Adheres to Compliance.

- B. Responds Courteously, Focuses on Customer, and Affirms the Customer.
- C. Uses Proper Grammar and Terms, Speaks Clearly, Shows a genuine interest to help.
- D. Overcomes Concerns, Portrays Positive Image, Asks Questions, Recommends Right Solution, and Ensures Satisfaction.
- E. Follows Training, Reviews Proper Info, Updates Proper Notes, Uses Proper Closing or Transfers to Correct Department.

**Quality Assurance Form Example – Standard Call Conversation**

#	Agent Name	First Name	Last Name	Phone Number	Recording DateTime	Disposition	Duration	Download
1	KristaCarey	Aaron	Rogers	4803898873	9/1/2020 11:45:14 AM	Call transferred to Bellevue	04:46	<a href="#">Download</a>
2	KristaCarey	Aaron	Rogers	4803898873	9/1/2020 11:48:01 AM	Call transferred to Bellevue	00:58	<a href="#">Download</a>
3	KristaCarey	Aaron	Rogers	4803898873	9/1/2020 11:45:28 AM	Call transferred to Bellevue	01:32	<a href="#">Download</a>

Questions	Answers	Comments
Did the agent start the conversation correctly ?	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Did the agent explain the purpose of the call ?	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Did our agent ask all the qualifying questions ?	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Did the agent make sure prospect stays on hold during transfer?	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Did our agent follow the Hand-Off script?	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Agent was answering questions
Disposition should be:	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Call transferred to Bellevue
<b>General Comments:</b>	Over all a great call	

[Submit](#)

Conversion Calls will partner with DHHS / ACCESSNebraska on this as we are flexible and customizable to meet your quality assurance form requirements.

As noted below, the initial training can be conducted directly by your team, or you can train our managers and supervisors and we'll train our team to save you time and resources (train the trainer model). From there, continuous improvement, on-going training, and development are all a part of our quality assurance process. We document electronically all observations, outcomes, feedback and coaching, and that information is fully accessible to the DHHS team.

### **Detailed Project Work Plan & Deliverables / Due Dates**

Conversion Call utilizes Agile Project Management methodology to ensure we will be flexible and customizable with DHHS while completing the project scope and objectives. We want to emphasize that we are not “cookie-cutter” and that we are here to be as useful as we can in support of ACCESSNebraska, your staff, and your citizens. We have a “no red tape” policy, work on the fly with you, and get the job done quickly. Our project leader and team will ensure your satisfaction and we are confident you will be impressed while receiving the ultimate benefit: Peace of Mind.

The project will be managed and completed through very talented, experienced and dedicated leaders and resources here at Conversion Calls. As noted, we focus on a delivery focused approach and therefore you will be assigned our CEO and CTO who both have over 16 years of implementing these exact call center and customer support solutions, and the other primary contact will be our Senior Vice President that is from Nebraska and has implemented many call center and customer support models, has utilized his project management certification and training, and we will use an Agile project management strategy to oversee the project solution, complete the scope of services and meet all deliverables and objectives on time. By using an Agile model, it allows us to be collaborative, maintain our flexibility and customization and deliver the solution quickly.



*We take every call personally*

For example, we will not wait to start on these deliverables until the contract is signed. We have started planning now no matter the outcome as it is a quick turn-around, and when the award notification is granted to us, we will instantly have the assigned team in place and executing decisions ahead of the actual contract signing. We can and will have up to 150 fully equipped, back-ground checked agents assigned or hired for this solution within seven days ready for systems access and training and can scale at this volume every seven days as well.

On the topic of training, we will partner with you to provide top-notch training, tools, and resources to promote success from the beginning whether your team trains them or you train our managers / supervisors, then we train the agent team, which we are glad to do and will save you time and resources. We will ensure access to a centralized and shared knowledge base and encourage and reinforce training opportunities through quality assurance in the spirit of continuous improvement at all times. One of our current best practices with CDLE is to conduct routine quizzes, knowledge tests, and internal “certifications” that are conducted on a weekly and/or monthly base to promote knowledge and process retention on previously trained items or integrating new program specific topics.

In most client partnerships, we both have Knowledge Bases that we both maintain and we share them in transparency. It’s all about communication and the appropriate training contacts and/or managers ensuring this information is updated, relevant, and accessible to all team members on both sides. Materials that are intended to for training will be utilized to do so and then will be added to the knowledge for future reference and reinforcement training. Our managers constantly coach, train, and remind our team members to utilize the Knowledge Base and know it well.

The DHHS / ACCESSNebraska personnel can update the Knowledge Base in real time and we will set up direct access to communicate to call center agents in real time as well. We do this now in partnership with our public / state agency clients.

### **Projected Timeline | Due Dates**

- Notice of Award, then signed contract.
- From signed contract a kick-off meeting will be scheduled within a few days to conduct intros, established key contacts, convey key tasks, timelines, and expectations.
- System access and/or integrations will be completed within two weeks.
- Agent team reassigned or hired and ready for training with management already in place within one week along with gathering training materials, accountabilities, and expectations.
- Training of team members is to be completed within 3 – 5 days. During this same time reporting and other benchmark tracking, telephony, system testing, and more is completed.
- Ready to go live in three weeks from signed contract.

We responded directly to deliverables and due dates above, however, at a higher-level Conversion Calls' implementation strategy is a form of concept mapping that includes:

- Training and Educating Stakeholders (DHHS / ACCESSNebraska and Conversion Calls and vice versa).
- Engaging and Supporting the Departments.
- Integrating the Infrastructure.
- Providing Proactive Assistance.

- Continue to Develop Stakeholder Relationships.
- Adapt and Tailor to the Client's and the Customer's Needs to Provide World-Class Customer Service and Operational Excellence.
- Evaluate Outcomes and Adjust as Recommended in Partnership with the Client.

As you review our response, you'll note that from a signed contract we project that we will be ready to go live in as soon as three weeks, or on a timeline of your preference as every client's need is different. For example, CDLE needed to be fully integrated and operational within 10 days and we accomplished that task with 100% success with over a hundred agent team members that we had ready for training within 7 days of signed contract and went live on day 10. From there we scale up and down for them on a weekly basis and have even provided up to 650+ agents during peak times. We are confident that we will meet & exceed your expectations based on our track record and experience.

### **REQUIRED BIDDER RESPONSES**

- Attachment #3 is completed in full and attached separately with the response.



## **COST PROPOSAL**

Conversion Calls is confident that our pricing is extremely competitive and at the same time DHHS / ACCESSNebraska will not sacrifice anything as we provide Peace of Mind. You will gain the following:

1. **Most likely better pricing**, which is budget friendly for the full contract term and allows DHHS / ACCESSNebraska to apply budget dollars toward other needs & priorities.
2. **A seamless and on-time transition**, and no sacrifice customer service, reporting, outcomes, data security, compliance, etc. We grant Peace of Mind for all of our client partners with our strong track record of success and vast higher ed and public government industry experience.
3. Flexibility, customization, and **strategic pivoting** is all included whether the request or service strategy is within or outside of the project scope. What we are emphasizing is that we do not “nickel and dime” our client-partners because our focus is to be a true partner as we will take you from your current state to your desired future state with 100% success.

**For example**, our dashboard and call analytics are unparalleled and our tech team just completed a three-week reporting and analytics customization project for one of our clients, Bellevue University, to transition them to a “future state”. We completed the request at no cost and the client was ecstatic with the outcome.

**Attachment #4 – “Cost Proposal Sheet” is completely filled out and attached separately, however, we want to highlight the following:**

- **No Set Up or Transition Fees.**
- **No Management Fees.**
- **No Integration or Programming Fees.**
- **We followed your template format, but you will calculate that our per call cost is broken down to about \$0.90 (90 cents) per minute.**
- **All technology, tech support, reporting, data analytics, customization, quality assurance, recordings, knowledge base, training and continuous training, and data and information security and compliance are included.**
- **All coverage for inbound or outbound calls is included.**
- **All requirements within the RFP will be met and exceeded, and all tasks required to take you from your current state to your desired future state with 100% satisfaction are included.**
- **All agents and team members are US Based, and pricing includes bilingual agents, all coverage hours including daytime hours, and any evening, night, and weekend differential hours that may be needed.**
- **Weekly scalability up or down meet call volumes throughout the yearly cycles (ie: we will scale the agent team up or down with a 7-day notice at any time).**

### **END RESULT**

- **Many organizations struggle with intangibles, but intangibles (ie: strategic solutions, innovation, knowledge, learning, communication) drive performance and growth, which DHHS / ACCESSNebraska gains as we take you from your current state to your desired future state with 100% success.**
- **True Partner with Strategic Solutions for you that meets and exceeds all RFP requirements and understands how to increase outcomes and desired results quickly at a competitive budget friendly price point.**
- **Innovation, Diversity, Flexibility, & Customization.**
- **World-Class Customer Service & Operational Excellence.**
- **Scalability Up and Down per your Organizational Needs Every 7 days.**
- **Outstanding Track Record and Outcomes Quickly as we partner with small, medium, large, and even larger clients than DHHS / ACCESSNebraska with complete satisfaction.**
- **Seamless Transition, and ultimate Peace of Mind.**

We are here to be true partners with DHHS / ACCESSNebraska and we ask that you communicate with us as to anything else we can do to meet and exceed your expectations as conversations move forward. On any topic...just ask!

## ATTACHMENT 3

### REQUIRED BIDDER RESPONSES

1.	<p>Describe your understanding of the business requirements, including reporting requirements. Describe your approach of how you will accomplish the business and reporting requirements.</p> <p>Bidder's Response: <b>Conversion Calls has thoroughly reviewed the business and reporting requirements on pages 30 and 31 of the primary RFP document and we fully understand and comply to meet and exceed the needs of the State of Nebraska, DHHS, AccessNebraska, and the citizens of Nebraska which includes programs such as Medicaid, SNAP, ADC, AABD, LIHEAP, State Disability, Child Care Subsidy, Refugee Resettlement Programs, and SSAD. All of our agents and team members are US Based as required and our approach of how we will accomplish the business and reporting requirements is as follows:</b></p> <p><b><u>Delivery-Focused Public Sector Approach:</u></b></p> <p>We differentiate ourselves from the competition in our delivery-focused approach instead of the typical sales-focused approach. Our leadership and managers are highly experienced with public / government organizations and contact center management as we have provided these services for over 16 years. We are committed and responsible individuals who have a service-oriented approach and put our client's interests ahead of our own as compared to other firms with sales-oriented Account Managers as their primary contact. Conversion Calls will assign a team specifically tasked with supporting your system, <b>your primary contact will be a senior leader that was raised, grew up and lived a few decades in Nebraska</b>, knows the area, knows the various communities, understands the cultures and the needs of citizens, and more. In addition, you will always have direct access to the CEO of Conversion Calls as we are available 24/7 and have a no red-tape policy (ie: we work quickly and will pivot quickly with you).</p> <p><b><u>Process-Driven Organization:</u></b></p> <p>Through our experience supporting large and diverse public government clients, Conversion Calls has honed our programs and processes to provide superior delivery and performance to our clients. Our mature operating protocol and processes are the cornerstone of our delivery model ensuring consistent delivery and quality across all verticals and geographies. We are confident in our abilities, and we will develop mutually beneficial metrics so that we deliver the same quality of service to the State of Nebraska – DHHS / AccessNebraska.</p> <p><b><u>Seamless Incumbent Transition:</u></b></p>
----	---

If needed and as appropriate, Conversion Calls understands that transitioning to or adding a new strategic partner demands a large effort, which in the beginning may require team members to operate differently than they did in the past. During this time, we need to keep stakeholders educated, motivated, and excited about the benefits we offer in both the short and long term. In order to accomplish this, Conversion Calls will partner with DHHS / AccessNebraska to develop a successful service solution that communicates and trains the team members efficiently and effectively.

**Proven Customized Recruiting and Screening:**

Conversion Calls has internal team members, bilingual operators, and maintains a pipeline of background checked candidates representing the required knowledge and skill set for this specific service that are all US Based (which is already a mandatory requirement at Conversion Calls). This pipeline planning greatly reduces our time to ensure the right team members by streamlining the process for our clients. In addition, we are glad to utilize willing incumbent team members as well and/or **assign or hire Nebraska residents too!**

**Public Government Sector Solution Provider:**

Our specific industry focus has given Conversion Calls the experience that allows us to quickly adapt to the state's needs, requirements, and preferences while also allowing us to invest in the right resources.

AccessNebraska can also leverage Conversion Calls' expertise in public sector contact center management to design, develop and manage strategies and effectively control the costs. In addition, several of our team members are bilingual and will be assigned accordingly, and our telephony and IT team of Five9 experts are extremely talented at call center and system integration and set up, programming IVRs, we utilize preferred numbers for all of our clients, provide full inbound and outbound call center agent customer service, provide all necessary equipment to be successful, provide call verification and qualification every day for all clients, provide all reporting, training, & quality assurance, call recording and archiving for up to seven years, texting is available through our Five9 system, and data pass-backs. All Service Requirements of inbound and outbound call coverage, email, etc, will be implemented with success and all staffing levels, on-call scheduling and rapid scalability on a week-to-week basis (vs monthly), schedules, and additional services will be maintained to achieve and exceed all service expectations highlighted in the RFP. Yes, we grant our

	<p>client partners peace of mind with scalability up or down with 7 days-notice as compared to typical 30 days-notice, which saves the organization a lot of money, is budget friendly, and you pay only for what you need.</p> <p><b><u>Client-Focused Customer Service:</u></b></p> <p>Above all, Conversion Calls strives to not only meet, but exceed all customer service needs. As our business partner, you will be our top priority as we are <b>flexible and customizable</b> in all we do within and outside of the scope. In other words, we will not nickel and dime you for customization requests or work done outside of the standard scope as most vendor-partners will do. For example, we just completed a three-week customization reporting request for a client in Nebraska at no additional charge. They were very appreciative of the “cost” and were ecstatic with the outcome.</p> <p>Starting with the personal attention of a senior leader, you will have a direct link to the Conversion Calls executive team and CEO keeping the lines of communication open and available at all times which means there is no red tape and minimal wait time as decisions and adjustments can be made almost instantly as we work on the fly and pivot quickly with all of our client partners.</p>
2.	<p>Describe your site security and how you will maintain security for remote workers. Both physical and technology security.</p> <p>Bidder's Response:  <b>All of our physical security, information security, disaster recovery policies and procedures and more are included in the various Conversion Calls data security documents that we have included with our response. We are fully compliant in all the areas that the RFP requires, which includes physical and data security, information security, PII, HIPPA, etc, and for public universities we are fully HECVAT approved as well. As mentioned, all of our agents and employees are US Based only, which is mandatory at Conversion Calls.</b></p>
3.	<p>Describe your language capabilities, including the percentage of call center staff who are bilingual in English and Spanish, and any other languages available. Describe how you will ensure that call center staff are able to communicate with individuals in multiple languages.</p> <p>Bidder's Response:  <b>About 25% of our call center staff is bilingual (English and Spanish). If there is a need for other languages to be supported, then like we do for our other public agency clients, we will utilize a language line to meet and exceed the expectation for all languages to be covered and fully serviced.</b></p>
4.	<p>Describe your experience handling Personal Protected Information (PPI) and Health Insurance Portability and Accountability Act (HIPAA) information, including any HIPAA training that employees have previously received. If you are a covered entity under HIPAA, please provide the number of breach notifications you reported to Office of Civil Rights in the last 3 years. If you are a business associate under HIPAA, please provide the number of security incidents which required notifications to Office of Civil Rights for any covered entities for which you are a business associate in the last three (3) years.</p> <p>Bidder's Response:  <b>Conversion Calls has had no (zero) breach notifications, security incidents, etc. We are highly experienced and compliant in handling PPI and meet HIPAA complaint standards as documented in our security documents which we included in our response. We are in</b></p>

	<p>partnership with other state agencies and support unemployment, benefit services, fraud prevention, public university services in the areas of student services, enrollment, financial aid, registrar services and more as we work with various residents for our clients that include students, parents, customers, claimants, family members, etc.</p>
5.	<p>Describe how you will securely print and mail documents.</p> <p>Bidder's Response:  <b>Conversion Calls will meet and exceed your requirements for a private and secure print and mail location as referenced and described in the RFP. We understand that print devices are considered work stations on HIPAA law, which means they fall under the same restrictions and requirements as other data storage and transfer devices. We will ensure that all passwords are updated and full network security is in place, the location and access will be secure at all times, we will initiate pull-printing via a PIN, electronic fax enablement can be set up if necessary, and all copier hard drives will be cleared in the event of a change. HIPAA rules state that all documents being mailed must be done through First Class mail or Certified mail, and the recipient must sign for it. Everything will be trackable and standard mail will never be utilized. Furthermore, we understand that the mailing/postage cost will be covered and refunded by AccessNebraska and in transparency we will forward those invoices and costs to you for reimbursement. Once again, Conversion Calls is US Based only and that applies to all employees and locations.</b></p>
6.	<p>Describe how you will ensure that any data resulting from services provided is properly secured according to the requirements in this RFP and is not used, accessed, or disseminated by any method or for any reason not authorized by DHHS.</p> <p>Bidder's Response:  <b>Conversion Calls will ensure that any and all data resulting from services provided is properly secured according to the RFP per all of our information data security documents that we provided with our response. We will meet and exceed your expectations in this area, we area as we do for other public client partners, we are fully compliant, and we are glad to go through monthly or routine certifications, audits, testing in these applicable areas. In addition, we review these mandatory requirements with all of our team members, have signed documentation, conduct background checks per client expectations, conduct quality assurance, routine training, observations, and more. It is mandatory that all employees are US Based and any data if applicable will always remain US Based at all times.</b></p>
7.	<p>Describe your ability to meet the facility requirements for the printing functions?</p> <p>Bidder's Response:  <b>All facility requirements for the printing functions will be fully met and exceeded per the RFP requirements. Conversion Calls is fully compliant and everyone and everything is 100% US Based. We understand that print devices are considered work stations on HIPAA law, which means they fall under the same restrictions and requirements as other data storage and transfer devices. We will ensure that all passwords are updated and full network security is in place, the location and access will be secure at all times, we will initiate pull-printing via a PIN, electronic fax enablement can be set up if necessary, and all copier hard drives will be cleared in the event of a change.</b></p>
8.	<p>Describe your approach to workforce planning, including the speed, agility, and flexibility necessary to match your workforce to the fluctuating demand of this contract. Response should include a description of equipment provided to staff.</p> <p>Bidder's Response:  <b>Conversion Calls provides peace of mind in this area for all of our clients because we pivot quickly as needed and we are always flexible and customizable in and out of project scope. We are here to be true partners and to be as useful and supportive as we can to the State of Nebraska, DHHS, and AccessNebraska. In addition, we extend our client partners the ability to scale agent need up or down with a 7 days-notice vs monthly like other vendor-partners, we have the capabilities to have up to 150 new hires or reassigned agents ready for training within seven days. Our agents are verified to have and/or provided the necessary equipment required to be successful such as laptops, highspeed internet, headsets, training and</b></p>

	<p>coaching, appropriate office environment, telephony, access to knowledgebase, and more. We want to emphasize that Conversion Calls has a “no red tape” policy, we work quickly, and make key decisions with you rapidly to ensure your expectations are met and exceeded in every area while providing world-class customer service and operational excellence.</p>
9.	<p>Describe your quality monitoring processes.</p> <p>Bidder’s Response:  <b>Conversion Calls has a substantial Quality Assurance process and monitoring system. Our goal is to observe, document, and provide coaching and training on approximately 25% of all calls. Everything is electronic and can be provided to the client at any time. <u>We have included a separate document with our response that provides visuals and more detail as to our quality assurance system and how it aligns to your example and expectations</u>, however, per quality assurance and training, attributes we observe, score, and hold team members accountable are:</b></p> <ul style="list-style-type: none"> <li>A. Proper Greeting, Identifies Self, Verifies Customer Info, Follows Scripting, and Adheres to Compliance.</li> <li>B. Responds Courteously, Focuses on Customer, and Affirms the Customer.</li> <li>C. Uses Proper Grammar and University Terms, Speaks Clearly, Shows a genuine interest to help.</li> <li>D. Overcomes Concerns, Portrays Positive Image, Asks Questions, Recommends Right Solution, and Ensures Satisfaction.</li> <li>E. Follows Training, Reviews Proper Info, Updates Proper Notes, Uses Proper Closing or Transfers to Correct Department.</li> </ul>
10.	<p>Describe your ability to meet the timelines established in this RFP for reporting and quality monitoring.</p> <p><b>Bidder’s Response:</b>  <b>The best and most resonating response we have is to provide an actual client example: We have a public state agency client that required us to provide 100 call center agents, managers, quality assurance set up, all telephony, all integrations &amp; access, security and compliance expectations in place, reporting, recordings, equipment needed to be successful, background checked, and ready for training within 7 days from a signed contract. We accomplished this requirement within 100% success. After an 18-month contract, due to our flexibility, customization, world-class customer service and operational excellence along with our outcomes, they extended with us for another five years.</b>  <b>This state agency is one of our references: Colorado Department of Labor &amp; Employment (CDLE) and they are currently a client-partner of ours. We have the ability and will meet the times established in the RFP for reporting, quality monitoring, and providing the agent team members, training, and all that you need on time.</b></p>
11.	<p>Describe your maximum call capacity and the timeframe required to increase call capacity.</p> <p><b>Bidder’s Response:</b>  <b>Our call capacity is unlimited (just communicate what you need at any time) and the timeframe required to increase call capacity is as referenced: a minimum of a 7 days-notice up or down scalability is what we are extending to you in our model. Its efficient, its cost effective, and its client / customer focused.</b></p>
12.	<p>Describe your capacity of in-house trainers and approach to on-boarding new call center staff to the project.</p>



	<p>Bidder's Response:  <b>As mentioned in response #1 &amp; #10, Conversion Calls has the capabilities and the track record to onboard new call center staff to the project quickly whether that is new-hires, reassignments, or even transferring incumbents as appropriate. We will onboard up to 150 agents every 7 days, and have them background checked, integrated, fully equipped, and ready for training within that 7 days. We actually begin this process prior to a signed contract if we have a verbal or emailed notification that we are the primary chosen vendor-partner to ensure we have everyone needed and in place on time while the contract process is finalizing. Our in-house trainers are already in place, we work with partners on train the trainer models to save time and resources for the client, we have knowledgebases we can utilize and/or continue to build, and will start the new agent training as agreed to with the client and have them ready to go live on time.</b></p>
13.	<p>Describe your staff retention policies and the average employee length of service.</p> <p>Bidder's Response:  <b>Average employee length of service at Conversion Calls is 2.25 years and our staff retention policies are: a) flexible schedule within the client needs, b) remote work options, c) culture of communication, recognition, and diversity d) family oriented / supportive, e) benefits and PTO, f) succession planning and promotion opportunities, g) solid training and equipping for success, h) weekly or bi-weekly pay options, i) leadership that cares and is friendly while having high expectations for our clients and customers, and j) we have fun!</b></p>
14.	<p>Describe your ability to meet the reporting requirements set forth in Section V.C.2. including ad hoc reporting capabilities.</p> <p>Bidder's Response:  <b>Conversion Calls has the ability, the experience, and the track record to meet all reporting requirements set forth in V.C.2. We are fully flexible and customizable in this area and meet and exceed ad hoc reporting requirements routinely for clients. In addition, anything that is needed whether it is in scope or out of scope we will complete for you within our proposal and ensure your complete satisfaction. <u>Bellevue University in Nebraska is one of our client-partners, and we just recently completed a three-week reporting customization project for them free of charge. They were very pleased with the outcome. The reporting requirements and examples you provided are absolutely no issue for us and will be matched or enhanced.</u></b></p>
15.	<p>Describe how DHHS staff will access your Automated Call Distribution (ACD) software to view real-time wait times and available call capacity.</p> <p>Bidder's Response:  <b>Conversion Calls will provide you viewable access to those systems and you will be able to access at anytime you'd like. In addition, we can provide reporting at any time and at any cadence to your preference as we always operate in transparency.</b></p>
16.	<p>Do you use an off the shelf Customer Relationship Management system, or one developed in house? If off the shelf, please specify the product and company. Please describe the capabilities of the Customer Relationship Management systems in use.</p> <p>Bidder's Response:  <b>Our internal CRM system was developed in-house by our very talented IT team. If needed, it is fully able to integrate and/or communicate with various client systems to ensure all data on the client side is updated, and stays on the client side per security and compliance requirements as we will not house the data in our systems. In fact, most of the time clients grant us secure access to their systems and our teams members update the data in real-time, or our IT team programs any data updates to take place daily in a secure system format of the client's preference. We are glad to discuss this further, but to-date for over 16 years, we have had no issues in this area with any of our clients as all have been completely satisfied.</b></p>

**ATTACHMENT 4  
COST PROPOSAL SHEET**

**Bidder Name**

**Conversion Calls LLC**

**ONE TIME COST**

Startup Plan/Implementation  
Cost

**\$0 No Startup charges**

**PASS THROUGH COSTS**

Cost per page, single sided  
printing

**\$ 0.20**

Training Cost Per Hour/Per  
Person

**\$24**

Note: Mailing cost will be reimbursed per current US Postal rates with no additional markup.

**COST PER CALL FOR INITIAL THREE YEAR PERIOD**

Service		Average Handled Time (AHT)	Number of calls/actions Tier I	Cost Per Call for Tier I	Number of calls/actions Tier II	Cost Per Call for Tier II	Number of calls/actions Tier III	Cost Per Call for Tier III
<b>Inbound</b>	A	11:00-15:00	6,000-16,999	\$ 13.44	17,000-27,999	\$ 15.22	28,000-40,000	\$ 17.00
	B	15:01-20:00	1,400-3,599	\$ 17.92	3,600-5,799	\$ 20.29	5,800-8,000	\$ 22.67
	C	20:01-25:00	1,400-3,599	\$ 22.40	3,600-5,799	\$ 25.37	5,800-8,000	\$ 28.33
	D	25:01-30:00	1,400-3,599	\$ 26.88	3,600-5,799	\$ 30.44	5,800-8,000	\$ 34.00
	E	30:01-35:00	1,400-3,599	\$ 31.36	3,600-5,799	\$ 35.51	5,800-8,000	\$ 39.66
<b>Outreach</b>	A	8:00 -12:00	1,400-3,599	\$ 10.75	3,600-5,799	\$ 12.18	5,800-8,000	\$ 13.60
	B	12:01 - 16:00	1,400-3,599	\$ 14.33	3,600-5,799	\$ 16.23	5,800-8,000	\$ 18.13
	C	16:01 - 20:00	1,400-3,599	\$ 17.92	3,600-5,799	\$ 20.29	5,800-8,000	\$ 22.67
<b>Back Office Processing</b>	A	4:00-8:00	1,400-3,599	\$ 7.17	3,600-5,799	\$ 8.12	5,800-8,000	\$ 9.07

B	8:01 - 12:00	1,400-3,599	\$ 10.75	3,600-5,799	\$ 12.18	5,800-8,000	\$ 13.60
C	12:01-16:00	1,400-3,599	\$ 14.33	3,600-5,799	\$ 16.23	5,800-8,000	\$ 18.13

**COST PER CALL FOR RENEWAL PERIOD 1**

Service		Average Handled Time (AHT)	Number of calls/actions Tier I	Cost Per Call for Tier I	Number of calls/actions Tier II	Cost Per Call for Tier II	Number of calls/actions Tier III	Cost Per Call for Tier III
Inbound	A	11:00-15:00	6,000-16,999	\$ 13.44	17,000-27,999	\$ 15.22	28,000-40,000	\$ 17.00
	B	15:01-20:00	1,400-3,599	\$ 17.92	3,600-5,799	\$ 20.29	5,800-8,000	\$ 22.67
	C	20:01-25:00	1,400-3,599	\$ 22.40	3,600-5,799	\$ 25.37	5,800-8,000	\$ 28.33
	D	25:01-30:00	1,400-3,599	\$ 26.88	3,600-5,799	\$ 30.44	5,800-8,000	\$ 34.00
	E	30:01-35:00	1,400-3,599	\$ 31.36	3,600-5,799	\$ 35.51	5,800-8,000	\$ 39.66
Outreach	A	8:00 -12:00	1,400-3,599	\$ 10.75	3,600-5,799	\$ 12.18	5,800-8,000	\$ 13.60
	B	12:01 - 16:00	1,400-3,599	\$ 14.33	3,600-5,799	\$ 16.23	5,800-8,000	\$ 18.13
	C	16:01 - 20:00	1,400-3,599	\$ 17.92	3,600-5,799	\$ 20.29	5,800-8,000	\$ 22.67
Back Office Processing	A	4:00-8:00	1,400-3,599	\$ 7.17	3,600-5,799	\$ 8.12	5,800-8,000	\$ 9.07
	B	8:01 - 12:00	1,400-3,599	\$ 10.75	3,600-5,799	\$ 12.18	5,800-8,000	\$ 13.60
	C	12:01-16:00	1,400-3,599	\$ 14.33	3,600-5,799	\$ 16.23	5,800-8,000	\$ 18.13

**COST PER CALL FOR RENEWAL PERIOD 2**

Service		Average Handled Time (AHT)	Number of calls/actions Tier I	Cost Per Call for Tier I	Number of calls/actions Tier II	Cost Per Call for Tier II	Number of calls/actions Tier III	Cost Per Call for Tier III
Inbound	A	11:00-15:00	6,000-16,999	\$ 13.44	17,000-27,999	\$ 15.22	28,000-40,000	\$ 17.00
	B	15:01-20:00	1,400-3,599	\$ 17.92	3,600-5,799	\$ 20.29	5,800-8,000	\$ 22.67
	C	20:01-25:00	1,400-3,599	\$ 22.40	3,600-5,799	\$ 25.37	5,800-8,000	\$ 28.33
	D	25:01-30:00	1,400-3,599	\$ 26.88	3,600-5,799	\$ 30.44	5,800-8,000	\$ 34.00
	E	30:01-35:00	1,400-3,599	\$ 31.36	3,600-5,799	\$ 35.51	5,800-8,000	\$ 39.66
Outreach	A	8:00 -12:00	1,400-3,599	\$ 10.75	3,600-5,799	\$ 12.18	5,800-8,000	\$ 13.60
	B	12:01 - 16:00	1,400-3,599	\$ 14.33	3,600-5,799	\$ 16.23	5,800-8,000	\$ 18.13
	C	16:01 - 20:00	1,400-3,599	\$ 17.92	3,600-5,799	\$ 20.29	5,800-8,000	\$ 22.67
Back Office Processing	A	4:00-8:00	1,400-3,599	\$ 7.17	3,600-5,799	\$ 8.12	5,800-8,000	\$ 9.07
	B	8:01 - 12:00	1,400-3,599	\$ 10.75	3,600-5,799	\$ 12.18	5,800-8,000	\$ 13.60
	C	12:01-16:00	1,400-3,599	\$ 14.33	3,600-5,799	\$ 16.23	5,800-8,000	\$ 18.13

### COST PER CALL FOR RENEWAL PERIOD 3

Service		Average Handled Time (AHT)	Number of calls/actions Tier I	Cost Per Call for Tier I	Number of calls/actions Tier II	Cost Per Call for Tier II	Number of calls/actions Tier III	Cost Per Call for Tier III
<b>Inbound</b>	A	11:00-15:00	6,000-16,999	\$ 13.44	17,000-27,999	\$ 15.22	28,000-40,000	\$ 17.00
	B	15:01-20:00	1,400-3,599	\$ 17.92	3,600-5,799	\$ 20.29	5,800-8,000	\$ 22.67
	C	20:01-25:00	1,400-3,599	\$ 22.40	3,600-5,799	\$ 25.37	5,800-8,000	\$ 28.33
	D	25:01-30:00	1,400-3,599	\$ 26.88	3,600-5,799	\$ 30.44	5,800-8,000	\$ 34.00
	E	30:01-35:00	1,400-3,599	\$ 31.36	3,600-5,799	\$ 35.51	5,800-8,000	\$ 39.66
<b>Outreach</b>	A	8:00 -12:00	1,400-3,599	\$ 10.75	3,600-5,799	\$ 12.18	5,800-8,000	\$ 13.60
	B	12:01 - 16:00	1,400-3,599	\$ 14.33	3,600-5,799	\$ 16.23	5,800-8,000	\$ 18.13
	C	16:01 - 20:00	1,400-3,599	\$ 17.92	3,600-5,799	\$ 20.29	5,800-8,000	\$ 22.67
<b>Back Office Processing</b>	A	4:00-8:00	1,400-3,599	\$ 7.17	3,600-5,799	\$ 8.12	5,800-8,000	\$ 9.07
	B	8:01 - 12:00	1,400-3,599	\$ 10.75	3,600-5,799	\$ 12.18	5,800-8,000	\$ 13.60
	C	12:01-16:00	1,400-3,599	\$ 14.33	3,600-5,799	\$ 16.23	5,800-8,000	\$ 18.13

## **FINANCIAL ATTESTATION**

I attest that Conversion Calls LLC is a financially viable and stable private company.

Conversion Calls LLC has all the adequate financial resources to support its proposal response and to provide all proposed services to Access Nebraska during the contract period.

Conversion Calls LLC financial status:

- Conversion Calls has been in business continuously for over 16 years.
- Conversion Calls has multi million annual revenue.
- Conversion Calls have been profitable since first year.
- Conversion Calls has zero debt or creditors.
- Conversion Calls has active contracts with The State of Colorado, and with multiple Colleges and Universities, promising future positive cash flow and stability for years to come.
- Conversion Calls is not involved in any lawsuits in the past or at present.
- Conversion Calls has sufficient liquid capital to meet all payroll and all operational expenses, as well as unexpected emergencies.

Shay Rosen  
CEO and Owner

*Shay Rosen*

December 5, 2022



**Report Criteria:**

*Start:* May 23, 2022 12:00:00 AM Mountain Standard Time

*End:* May 29, 2022 11:58:00 PM Mountain Standard Time

*Speed of answer* 0

*minimum time:*

*Service Level:* 20

CALL TYPE	DISPOSITION	DATE							
		2022/05/23	2022/05/24	2022/05/25	2022/05/26	2022/05/27	2022/05/28	2022/05/29	TOTAL
		CALLS	CALLS	CALLS	CALLS	CALLS	CALLS	CALLS	CALLS
3rd party conference	-		-	-	-	-	-	-	1
3rd party transfer	-								
Queue Callback	-								
Inbound	Abandon								
Inbound	Agent Error								
Inbound	Call Received After Hours								
Inbound	Caller Disconnected								
Inbound	Caller Disconnected.								
Manual	Caller Disconnected.								
Inbound	General Questions								
Inbound	ID.me completed - payment still on hold								
Inbound	Incomplete Claim								
Internal	Internal Call								
Inbound	New Claim								
Inbound	No Disposition								
Inbound	Password Reset Request								
Inbound	Program Integrity								
Inbound	Reopened Claim								
Inbound	Timeout								
Inbound	Transferred To 3rd Party								
Inbound	Weekly Claim								
Manual	Weekly Claim								





**Report Criteria:**

*Start:* May 23, 2022 12:00:00 AM Mountain Standard Time

*End:* May 29, 2022 11:59:00 PM Mountain Standard Time

*Speed of answer 0  
minimum time:*

*Service Level: 20*

CALL TIME	BILL TIME (ROUNDED)	COST	IVR TIME	QUEUE WAIT TIME	TALK TIME

**Report Criteria:**

*Start:* May 23, 2022 12:00:00 AM Mountain Standard Time

*End:* May 29, 2022 11:58:00 PM Mountain Standard Time

*Agent State:* After Call Work, Login, Not Ready, On Call, On Preview, On Voicemail, Ready, Ringing

*Long Calls:* 600

*Short Calls:* 10

*Long Parks:* 300

*Long Holds:* 300

*Long After Call Work:* 600

*Short After Call Work:* 0

DATE	LOGIN TIME	Average LOGIN TIME	READY TIME	Average READY TIME	ON CALL TIME	Average ON CALL TIME

**Report Criteria:**

*Start:* May 16, 2022 12:00:00 AM Mountain Standard Time

*End:* May 22, 2022 11:58:00 PM Mountain Standard Time

*Campaign:* ConversionCalls Inbound CDLE English, ConversionCalls Inbound CDLE Spanish

*Speed of answer* 0

*minimum time:*

*Service Level:* 20

HALF HOUR	CALLS	CALLS (%grp)	CALL TIME	Average CALL TIME	COST	Average COST
00:00						
00:30						
01:00						
01:30						
02:00						
02:30						
03:00						
03:30						
04:00						
04:30						
05:00						
05:30						
06:00						
06:30						
07:00						
07:30						
08:00						
08:30						
09:00						
09:30						
10:00						
10:30						
11:00						
11:30						
12:00						
12:30						
13:00						
13:30						
14:00						
14:30						
15:00						
15:30						
16:00						

W - Calls By Time Of Day - CDLE

---

16:30	
17:00	
17:30	
18:00	
18:30	
19:00	
19:30	
20:00	
20:30	
21:00	
21:30	
22:00	
22:30	
23:00	
23:30	



*We take every call personally*

## Data Privacy Policy

### Overview

Data privacy is a critical component of Conversion Calls operations. The protection and management of the various types of student and staff Personally Identifiable Information (PII) is critical to Conversion Calls. Our computer systems and related devices collect and record data as required for educational delivery, management, and reporting purposes. This key information should never be disclosed to unauthorized individuals.

### Purpose

This policy establishes general privacy requirements for information captured or generated by Conversion Calls operations, systems, network devices, or communications. This includes systems and devices involved in the transmission and storage of voice data. The policy further delimits conditions where PII may be disclosed.

### Scope

This policy applies to all Conversion Calls staff that create, deploy, or support Conversion Calls gathered or processed information.

### Policy

## GENERAL STATEMENT OF STUDENT DATA PRIVACY

Conversion Calls policy surrounding data privacy falls into three broad classifications protecting information gathered to manage and deliver services to employees, students, and districts. This policy is broken into three separate sections – general network data, PII, and employee information.

Using data effectively and responsibly is foundational to making the best decisions in today's schools about improving student performance. The Family Educational Rights Privacy Act (FERPA) and other state or federal laws establish baseline parameters for what is permissible when sharing student PII.

Conversion Calls uses additional guidelines and strict processes to protect the privacy of every student and ensure the confidentiality and security of all PII collected and managed.

## GENERAL NETWORK DATA

In the course of normal network operations, computer systems, voice systems, access control systems, and network devices generate and track logging data, source and destination internet protocol (IP) addresses, session times, port numbers, file sizes, etc. (referenced as Network Data).

- **Network Data Policy** - Conversion Calls treats all network data as confidential information. This information may be obtained, stored, and



*We take every call personally*

reported for legitimate business, compliance and audit purposes but shall not be exposed to unauthorized individuals except as specifically discussed in this policy.

- Network data may be disclosed under the following conditions.  
Requests shall be authorized by the IT Manager or their designee:
- **Network Operational Viability** - Network data may be released under the following situations:
  - Network performance monitoring or troubleshooting
  - Security incident analysis and remediation
  - Audit, group policy, and security log management and analysis
  - Litigation holds and requests
  - Copying, archiving, or otherwise preserving portions of any messages transmitted over the network in the course of business or maintenance
- **Legal or Conversion Calls Policy Analysis** – Network data may be released to appropriate authorities to indicate the presence of activities that violate internal policies, federal or state law. These requests shall be in response to legal discovery or court requests.
- **Network Security Threats** – All relevant data, protocol, logs, and user information may be released as part of incident and breach analysis and remediation. Conversion Calls shall investigate and remediate possible network security threats by means of capturing logging, and examination of files, communications, and other traffic and transmissions over or on the network.
- **Network Data Requests** - All requests to retrieve and share network data must be submitted to the IT Manager or their designee. Any litigation and legal requests require confirmation by both the CEO and CTO. Such requests shall include:
  - Name and role of the requestor.
  - Reason for the request, in accordance with the principles set forth in this policy.
  - Intended use of the requested data.
  - Any network data intentionally shared with third parties must be sanitized and redacted to preserve the anonymity of network users unless that data is used directly in legal discovery or authorized by



*We take every call personally*

general counsel and the CTO. Requests shall be documented and stored as part of the implementation of this policy.

## **EMPLOYEE DATA**

All employee data is treated as confidential and private. No employee related information shall be released or disclosed without the express approval of Conversion Calls IT Management Team.

**Employee Data Policy** - Conversion Calls treats all employee data as private and confidential information. This information may be obtained, stored, and reviewed for legitimate business purposes related to personnel employment, compliance, and audit purposes but shall not be exposed to unauthorized individuals, agencies, or external sources except as specifically discussed in this policy.

Requests shall be authorized by the IT Manager in concert with the CTO when electronic records are involved. Data shall be disclosed only under the following conditions and employees shall be informed of such activity prior to release:

- **Employee Performance or Transitions** – Employee work data may be released under the following situations:
  - Security incident analysis and remediation
  - Litigation holds and requests
  - Personnel transitions involving email and work products
  - Restoration or otherwise preserving portions of messages transmitted over the network in the course of business.
- **Legal or Agency Disciplinary Analysis** – Employee data may be released to appropriate authorities to indicate the presence of activities that violate internal policies, federal or state law. These requests shall be in response to internal policy incidents, personnel management, legal discovery, or court requests.
- **Network or Agency Security Threats** – All relevant data, protocol, logs and user information may be released as part of incident and breach analysis and remediation. Conversion Calls shall investigate and remediate possible network security threats by means of capture, logging, and examination of files, communications, and other traffic and transmissions over or on the network including all employee communications and component activities relevant to the incident or breach.
- **Employee Data Requests** - All requests to retrieve and share employee data must be submitted through the Conversion Calls IT Team. Any litigation and legal requests require confirmation by executive management including at a minimum the CTO. Such requests shall include:





*We take every call personally*

- Name and role of the requestor.
- Reason for the request, in accordance with the principles set forth in this policy.
- Intended use of the requested data and whether this information will be used as part of a personnel action.
- Employee notification of the event unless barred due legal or disciplinary investigation. In all circumstances, employees shall be notified if information is placed in their permanent files related to an incident or discovery request.

Any employee network data intentionally shared with third parties shall be sanitized and redacted to preserve the anonymity of the employee unless that data is used directly in legal discovery or authorized by the Conversion Calls General Counsel. Requests shall be documented and stored as part of the implementation of this policy.

### **Audit Controls and Management**

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of Conversion Calls operations. Examples of audit control and evidence include:

- Process, authorizations, and documentation for PII requests
- Historical evidence or organizational compliance
- Functioning IRB and research authorization process and regular evidence of board activity
- Procedures for executing legal holds, chain of command, and discovery requests

### **Enforcement**

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

### **Distribution**

This policy is to be distributed to all Conversion Calls staff.



*We take every call personally*

## **Information security policy**

### **1.Overview**

Conversion Calls's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Conversion Calls's established culture of openness, trust and integrity. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Conversion Calls. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations..

Effective security is a team effort involving the participation and support of every Conversion Calls employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

### **2.Purpose**

The purpose of this policy is to outline the acceptable use of computer equipment at Conversion Calls. These rules are in place to protect the employee and Conversion Calls. Inappropriate use exposes Conversion Calls to risks including virus attacks, compromise of network systems and services, and legal issues.

### **3.Scope**

This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by Conversion Calls, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Conversion Calls and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Conversion Calls policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Conversion Calls, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Conversion Calls.

## 4. Policy

### 4.1 General Use and Ownership

- 4.1.1 Conversion Calls proprietary information stored on electronic and computing devices whether owned or leased by Conversion Calls, the employee or a third party, remains the sole property of Conversion Calls. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard*.
- 4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Conversion Calls proprietary information.
- 4.1.3 You may access, use or share Conversion Calls proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- 4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- 4.1.5 For security and network maintenance purposes, authorized individuals within Conversion Calls may monitor equipment, systems and network traffic at any time, per Conversion Calls's Audit Policy.
- 4.1.6 Conversion Calls reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

### 4.2 Security and Proprietary Information

- 4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.
- 4.2.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- 4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.



*We take every call personally*

- 4.2.4 Postings by employees from a Conversion Calls email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Conversion Calls, unless posting is in the course of business duties.
- 4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

### **4.3 Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Conversion Calls authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Conversion Calls owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

#### **4.3.1 System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Conversion Calls.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Conversion Calls or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting Conversion Calls business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).



*We take every call personally*

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Conversion Calls computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Conversion Calls account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to Conversion Calls is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the Conversion Calls network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Conversion Calls employees to parties outside Conversion Calls.



*We take every call personally*

#### 4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Conversion Calls's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Conversion Calls or connected via Conversion Calls's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

#### 4.3.3 Blogging and Social Media

1. Blogging by employees, whether using Conversion Calls's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Conversion Calls's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Conversion Calls's policy, is not detrimental to Conversion Calls's best interests, and does not interfere with an employee's regular work duties. Blogging from Conversion Calls's systems is also subject to monitoring.
2. Conversion Calls's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Conversion Calls's Confidential Information policy when engaged in blogging.



*We take every call personally*

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Conversion Calls and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Conversion Calls's Non-Discrimination and Anti-Harassment policy.
4. Employees may also not attribute personal statements, opinions or beliefs to Conversion Calls when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Conversion Calls. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Conversion Calls's trademarks, logos and any other Conversion Calls intellectual property may also not be used in connection with any blogging activity

## **5. Policy Compliance**

### 5.1 Compliance Measurement

The Conversion Calls team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

### 5.2 Exceptions

Any exception to the policy must be approved by the Conversion Calls team in advance.

### 5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.



*We take every call personally*

# IT Disaster Recovery Plan



## Table of Contents

Information Technology Statement of Intent	5
Policy Statement	5
Objectives	5
Key Personnel Contact Info	6
Notification Calling Tree	7
External Contacts	8
1 Plan Overview	9
1.1 Plan Updating	9
1.2 Plan Documentation Storage	9
1.3 Backup Strategy	9
1.4 Risk Management	10
2 Emergency	11
2.1 Alert, escalation and plan invocation	11
2.1.1 Plan Triggering Events	11
2.2.2 Assembly Points	11
2.2.3 Activation of Emergency Response Team	11
2.3 Disaster Recovery Team	11
2.4 Emergency Alert, Escalation and DRP Activation	12
2.4.1 Emergency Alert	12
2.4.2 DR Procedures for Management	13
2.4.3 Contact with Employees	13
2.4.4 Backup Staff	13
2.4.5 Recorded Messages / Updates	13

2.3.7	Alternate Recovery Facilities / Hot Site	14
2.3.8	Personnel and Family Notification	14
3	Media	14
3.1	Media Contact	14
3.2	Media Strategies	14
3.3	Media Team	14
3.4	Rules for Dealing with Media	15
4	Financial and Legal Issues	16
4.1	Financial Assessment	16
4.2	Financial Requirements	16
4.3	Legal Actions	16
5	DRP Exercising	17
Appendix A – Technology Disaster Recovery Plan		18
Disaster Recovery Plan		18
Disaster Recovery Plan for Local Area Network (LAN)		20
Appendix B – Suggested Forms		22
Disaster Recovery Event Recording Form		23
Disaster Recovery Activity Report Form		23
Mobilizing the Disaster Recovery Team Form		24
Mobilizing the Business Recovery Team Form		24
Monitoring Business Recovery Task Progress Form		25
Preparing the Business Recovery Report Form		26
Communications Form		26
Returning Recovered Business Operations to Business Unit Leadership		27
Business Process/Function Recovery Completion Form		27

## Information Technology Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

## Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

## Objectives

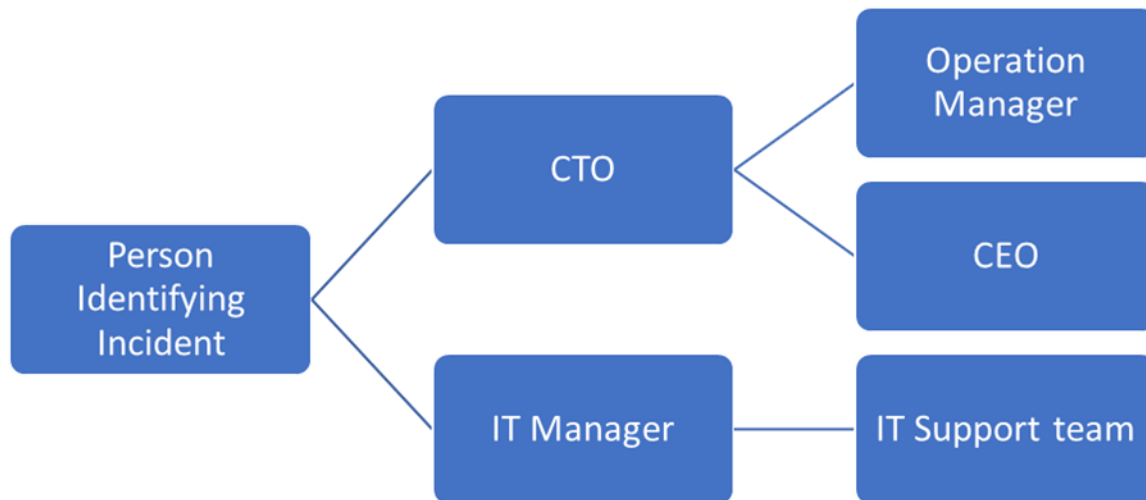
The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites

### Key Personnel Contact Info

Name, Title	Contact Option	Contact Number
Neil Netivi, CTO	Work	954-607-2021
	Alternate	
	Mobile	786-271-7496
	Home	
	Email Address	neiln@conversioncalls.com
	Alternate Email	
Shay Rosen, CEO	Work	954-607-2019
	Alternate	
	Mobile	954-608-5391
	Home	
	Email Address	srosen@conversioncalls.com
	Alternate Email	
Matt Hanusa, Senior Vice President	Work	954-607-1990 Ext. 110
	Alternate	
	Mobile	913-209-2502
	Home	
	Email Address	mhanusa@conversioncalls.com
	Alternate Email	
Patrick Michaels, IT Manager	Work	954-507-3506
	Alternate	
	Mobile	305-934-0444
	Home	
	Email Address	pmichaels@conversioncalls.com
	Alternate Email	

## Notification Calling Tree



**External Contacts**

<b>Name, Title</b>	<b>Contact Option</b>	<b>Contact Number</b>
<b>Landlord / Property Manager</b>		
Benjamin		
	Work	305-606-3480
	Mobile	
	Home	
	Email Address	
<b>Server Hosting</b>		
	Work	888-865-4261
Gadi	Mobile	954-818-4790
	Fax	
	Email Address	<a href="mailto:support@volico.com">support@volico.com</a>

## Plan Overview

### 1.1 *Plan Updating*

It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the IT Director.

### 1.2 *Plan Documentation Storage*

Copies of this Plan, CD, and hard copies will be stored in secure locations to be defined by the company. Each member of senior management will be issued a CD and hard copy of this plan to be filed at home. Each member of the Disaster Recovery Team and the Business Recovery Team will be issued a CD and hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

### 1.3 *Backup Strategy*

Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is for a fully mirrored recovery site at the company's offices in

This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site (headquarters) and the backup site.

<b>KEY BUSINESS PROCESS</b>	<b>BACKUP STRATEGY</b>
IT Operations	Fully mirrored recovery site
Tech Support - Hardware	Fully mirrored recovery site
Tech Support - Software	Fully mirrored recovery site
Facilities Management	Fully mirrored recovery site
Email	Fully mirrored recovery site
Disaster Recovery	Fully mirrored recovery site
Finance	Fully mirrored recovery site
Contracts Admin	Fully mirrored recovery site

Maintenance Sales	Fully mirrored recovery site
Human Resources	Off-site data storage facility
Call Center	Fully mirrored recovery site
Web Site	Fully mirrored recovery site

## 1.4 *Risk Management*

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Flood	3	4	All critical equipment is located on 1st Floor
Fire	3	4	FM200 suppression system installed in main computer centers. Fire and smoke detectors on all floors.
Tornado	5		Shutters installation
Electrical storms	5		Contact FPL
Act of terrorism	5		Contact local authorities
Act of sabotage	5		Contact police
Electrical power Failure	3	4	Redundant UPS array together with auto standby generator that is tested weekly & remotely monitored 24/7. UPSs also remotely monitored.
Loss of communications network services	4	4	Two diversely routed T1 trunks into building. WAN redundancy, voice network resilience

Probability: 1=Very High, 5=Very Low

Impact: 1=Total destruction, 5=Minor annoyance



## 2 Emergency

### 2.1.1 *Alert, escalation and plan invocation*

#### 2.1.2 *Plan Triggering Events*

2.2 Key trigger issues at headquarters that would lead to activation of the DRP are:

- Total loss of all communications
- Total loss of power
- Flooding of the premises
- Loss of the building

### 2.2.2 *Assembly Points*

Where the premises need to be evacuated, the DRP invocation plan identifies two evacuation assembly points:

- Primary – Far end of main parking lot;
- Alternate – Parking lot of company across the street

### 2.2.3 *Activation of Emergency Response Team*

When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a Quick Reference card containing ERT contact details to be used in the event of a disaster.

Responsibilities of the ERT are to:

- Respond immediately to a potential disaster and call emergency services;
- Assess the extent of the disaster and its impact on the business, data center, etc.;
- Decide which elements of the DR Plan should be activated;
- Establish and manage disaster recovery team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required

## 2.3 *Disaster Recovery Team*

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within 2.0 business hours;
- Restore key services within 4.0 business hours of the incident;
- Recover to business as usual within 8.0 to 24.0 hours after the incident;
- Coordinate activities with the disaster recovery team, first responders, etc.
- Report to the emergency response team

## 2.4 *Emergency Alert, Escalation and DRP Activation*

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

### 2.4.1 *Emergency Alert*

The person discovering the incident calls a member of the Emergency Response Team in the order listed:

Emergency Response Team

- Neil Netivi
- Patrick Michaels

If not available try:

- Shay Rosen
- Matt Hanusa

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated. The Business Recovery Team (BRT) will consist of senior representatives from the main business departments. The BRT Leader will be a senior member of the company's management team, and will be responsible for taking overall charge of the process and ensuring that the company returns to normal working operations as early as possible.

### ***2.4.2 DR Procedures for Management***

Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a hard copy of the company's disaster recovery and business continuity plans on file in their homes in the event that the headquarters building is inaccessible, unusable, or destroyed.

### ***2.4.3 Contact with Employees***

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster.

### ***2.4.4 Backup Staff***

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

### ***2.4.5 Recorded Messages / Updates***

For the latest information on the disaster and the organization's response, staff members can call a toll-free hotline listed in the DRP wallet card. Included in messages will be data on the nature of the disaster, assembly sites, and updates on work resumption.

### ***2.3.7 Alternate Recovery Facilities / Hot Site***

If necessary, the hot site at SunGard will be activated and notification will be given via recorded messages or through communications with managers. Hot site staffing will consist of members of the disaster recovery team only for the first 24 hours, with other staff members joining at the hot site as necessary.

### ***2.3.8 Personnel and Family Notification***

If the incident has resulted in a situation which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

## **3 Media**

### ***3.1 Media Contact***

Assigned staff will coordinate with the media, working according to guidelines that have been previously approved and issued for dealing with post-disaster communications.

### ***3.2 Media Strategies***

1. Avoiding adverse publicity
2. Take advantage of opportunities for useful publicity
3. Have answers to the following basic questions:
  - What happened?
  - How did it happen?
  - What are you going to do about it?

### ***3.3 Media Team***

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

### **3.4 *Rules for Dealing with Media***

**Only** the media team is permitted direct contact with the media; anyone else contacted should refer callers or in-person media representatives to the media team.

## **4 Financial and Legal Issues**

### **4.1 *Financial Assessment***

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment should include:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.
- Loss of cash

### **4.2 *Financial Requirements***

The immediate financial needs of the company must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post- disaster

### **4.3 *Legal Actions***

The company legal department and ERT will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

## ***5   DRP Exercising***

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens

## Appendix A – Technology Disaster Recovery Plan

### Disaster Recovery Plan

<b>SYSTEM</b>	
---------------	--

<b>OVERVIEW</b>	
<b>PRODUCTION SERVER</b>	Location: <b>Coral Springs FL</b> Server Model: <b>Dell</b> Operating System: Windows 2012 CPUs: 4 Memory: 30 GB Total Disk: 2 System Handle: IP Address: 173.24.6.52.98

<b>KEY CONTACTS</b>	
Hardware Vendor	Volico Inc
System Owners	Volico Inc
Database Owner	Conversion Calls
Application Owners	Conversion Calls
Offsite Storage	Volico Inc

<b>BACKUP STRATEGY FOR SYSTEM ONE</b>	
Daily	x
Monthly	x
Quarterly	x
<b>SYSTEM ONE DISASTER RECOVERY PROCEDURE</b>	
<u>Scenario 1</u>	Database Restore to original location
Total Loss of Data	



## File Systems

File System as of	File system Mounted on	Kbytes	Used	Avail	%used
Minimal file systems to be created and restored from backup:	Coldfusion Server Database Server				
Critical files to restore	CFM Files, Database files				

**Disaster Recovery Plan for Local Area Network (LAN)**

<b>SYSTEM</b>	
---------------	--

<b>OVERVIEW</b>	
<b>SERVER</b>	Location: <b>Office</b> Server Model: <b>Dell</b> Operating System: Windows <b>2019</b> CPUs:4 Memory: 16GB

<b>KEY CONTACTS</b>	
Hardware Vendor	Dell
System Owners	Conversion Calls
Database Owner	Conversion Calls
Application Owners	Conversion Calls
Software Vendors	Conversion Calls

<b>BACKUP STRATEGY for SYSTEM TWO</b>	
Daily	x
Monthly	x
Quarterly	x

<b>SYSTEM TWO DISASTER RECOVERY PROCEDURE</b>	
<u>Scenario 1</u>	Domain Server Restore File Server Restore
Total Loss of Data	



*We take every call personally*

**ADDENDUM**

<b>CONTACTS</b>	
Patrick Michaels	IT Manager
Neil Netivi	CTO

## Appendix B

### Damage Assessment Form

Key Business Process Affected	Description Of Problem	Extent Of Damage

### Management of DR Activities Form

- ☐ During the disaster recovery process all activities will be determined using a standard structure;
- ☐ Where practical, this plan will need to be updated on a regular basis throughout the disaster recovery period;
- ☐ All actions that occur during this phase will need to be recorded

<b>Activity Name:</b>
<b>Reference Number:</b>
<b>Brief Description:</b>

Commencement Date/Time	Completion Date/Time	Resources Involved	In Charge

## Disaster Recovery Event Recording Form

- ☐ All key events that occur during the disaster recovery phase must be recorded.
- ☐ An event log shall be maintained by the disaster recovery team leader.
- ☐ This event log should be started at the commencement of the emergency and a copy of the log passed on to the business recovery team once the initial dangers have been controlled.
- ☐ The following event log should be completed by the disaster recovery team leader to record all key events during disaster recovery, until such time as responsibility is handed over to the business recovery team.

<b>Description of Disaster:</b>
<b>Commencement Date:</b>
<b>Date/Time DR Team Mobilized:</b>

Activities Undertaken by DR Team	Date and Time	Outcome	Follow-On Action Required

<b>Disaster Recovery Team's Work Completed:</b> <Date>
<b>Event Log Passed to Business Recovery Team:</b> <Date>

## Disaster Recovery Activity Report Form

- ☐ On completion of the initial disaster recovery response the DRT leader should prepare a report on the activities undertaken.
- ☐ The report should contain information on the emergency, who was notified and when, action taken by members of the DRT together with outcomes arising from those actions.
- ☐ The report will also contain an assessment of the impact to normal business operations.
- ☐ The report should be given to business recovery team leader, with a copy to senior management, as appropriate.
- ☐ A disaster recovery report will be prepared by the DRT leader on completion

of the initial disaster recovery response.

- ☐ In addition to the business recovery team leader, the report will be distributed to senior management

The report will include:

- ☐ A description of the emergency or incident
- ☐ Those people notified of the emergency (including dates)
- ☐ Action taken by members of the DRT
- ☐ Outcomes arising from actions taken
- ☐ An assessment of the impact to normal business operations
- ☐ Assessment of the effectiveness of the BCP and lessons learned
- ☐ Lessons learned

### Mobilizing the Disaster Recovery Team Form

- ☐ Following an emergency requiring recovery of technology infrastructure assets, the disaster recovery team should be notified of the situation and placed on standby.
- ☐ The format shown below can be used for recording the activation of the DR team once the work of the damage assessment and emergency response teams has been completed

<b>Description of Emergency:</b>					
Date Occurred:					
Date Work of Disaster Recovery Team Completed:					
Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g., Specific Instructions Issued)					

### Mobilizing the Business Recovery Team Form

- ☐ Following an emergency requiring activation of the disaster recovery team, the business recovery team should be notified of the situation and placed on standby.

*We take every call personally*

- ❑ The format shown below will be used for recording the activation of the business recovery team once the work of the disaster recovery team has been completed.

<b>Description of Emergency:</b>					
Date Occurred:					
Date Work of Business Recovery Team Completed:					
Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g., Specific Instructions Issued)					

### Monitoring Business Recovery Task Progress Form

- ❑ The progress of technology and business recovery tasks must be closely monitored during this period of time
- ❑ Since difficulties experienced by one group could significantly affect other dependent tasks it is important to ensure that each task is adequately resourced and that the efforts required to restore normal business operations have not been under estimated

*Note: A priority sequence must be identified although, where possible, activities will be carried out simultaneously.*

Recovery Tasks (Order of Priority)	Person(s) Responsible	Completion Date		Milestone Identified	Other Relevant Information
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					

## Preparing the Business Recovery Report Form

- ☐ On completion of business recovery activities the BRT leader should prepare a report on the activities undertaken and completed
- ☐ The report should contain information on the disruptive event, who was notified and when, action taken by members of the BRT together with outcomes arising from those actions
- ☐ The report will also contain an assessment of the impact to normal business operations
- ☐ The report should be distributed to senior management, as appropriate

The contents of the report shall include:

- ☐ A description of the incident
- ☐ People notified of the emergency (including dates)
- ☐ Action taken by the business recovery team
- ☐ Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Problems identified
- Suggestions for enhancing the disaster recovery and/or business continuity plan
- Lessons learned

## Communications Form

- It is very important during the disaster recovery and business recovery activities that all affected persons and organizations are kept properly informed
- The information given to all parties must be accurate and timely
- In particular, any estimate of the timing to return to normal working operations should be announced with care
- It is also very important that only authorized personnel deal with media queries



Groups of Persons or Organizations Affected by Disruption	Persons Selected To Coordinate Communications to Affected Persons / Organizations		
	Name	Position	Contact Details
Customers			
Management & Staff			
Suppliers			
Media			
Stakeholders			
Others			

## Returning Recovered Business Operations to Business Unit Leadership

- Once normal business operations have been restored it will be necessary to return the responsibility for specific operations to the appropriate business unit leader
- This process should be formalized in order to ensure that all parties understand the change in overall responsibility, and the transition to business- as-usual
- It is likely that during the recovery process, overall responsibility may have been assigned to the business recovery process lead
- It is assumed that business unit management will be fully involved throughout the recovery, but in order for the recovery process to be fully effective, overall responsibility during the recovery period should probably be with a business recovery process team

### Business Process/Function Recovery Completion Form

The following transition form should be completed and signed by the business recovery team leader and the responsible business unit leader, for each process recovered.

A separate form should be used for each recovered business process.



*We take every call personally*

<b>Name Of Business Process</b>	
<b>Completion Date of Work Provided by Business Recovery Team</b>	
<b>Date of Transition Back to Business Unit Management</b> <i>(If different than completion date)</i>	
<p>I confirm that the work of the business recovery team has been completed in accordance with the disaster recovery plan for the above process, and that normal business operations have been effectively restored.</p> <p>Business Recovery Team Leader Name: _____</p> <p>Signature: _____ Date: _____</p> <p>_____</p> <p><i>(Any relevant comments by the BRT leader in connection with the return of this business process should be made here.)</i></p>	
<p>I confirm that above business process is now acceptable for normal working conditions.</p> <p>Name: _____ Title: _____</p> <p>Signature: _____</p> <p>Date: _____</p>	



*We take every call personally*

## **Physical Security Policy**

### **Overview**

A Physical Security policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

## **1.Purpose**

The purpose for this policy is to establish the minimum requirements for maintaining a "Physical Security" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Physical Security policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

## **2.Scope**

This policy applies to all Conversion Calls employees and affiliates.

## **3.Policy**

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when the workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the work day.



*We take every call personally*

- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

## **4. Policy Compliance**

### Compliance Measurement

The Conversion Calls team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.



*We take every call personally*

### Exceptions

Any exception to the policy must be approved by the Conversion Calls team in advance.

### Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.



February 10, 2021

Conversion Calls  
1830 N University Dr  
Plantation, FL 33322

Dear Neil Netivi:

We have received your request for information regarding material changes in internal control related to the co-location services offered to Conversion Calls. A-Lign prepared the latest Type II SOC 2 examination performed under AT section 101, Attest Engagements. This report includes tests of operating effectiveness for the period July 1, 2018 through January 31, 2019. Volico, as a normal part of its operations, continually updates its services and technology as appropriate. Volico recognizes the need to maintain an appropriate internal control environment and report upon the effectiveness, as well as material changes to its internal controls. As of February 10, 2021, I am not aware of any material changes in our control environment that would adversely affect the Auditor's Opinion reached in the 2020 report for the above named SOC 2.

Sincerely,



Gadi Hus  
Director of Operations



A-LIGN



VOLICO Enterprise  
Hosting Solutions  
Type 2 SOC 2  
2019



**REPORT ON VOLICO ENTERPRISE HOSTING SOLUTIONS' DESCRIPTION OF ITS  
SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING  
EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY AND  
AVAILABILITY**

**Pursuant to Reporting on System and Organization Controls 2 (SOC 2)  
Type 2 examination performed under AT-C 105 and AT-C 205**

**July 1, 2018 To January 31, 2019**



## Table of Contents

<b>SECTION 1 MANAGEMENT OF VOLICO ENTERPRISE HOSTING SOLUTIONS' ASSERTION REGARDING ITS SYSTEM THROUGHOUT THE PERIOD JULY 1, 2018 TO JANUARY 31, 2019.....</b>	<b>1</b>
<b>SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT .....</b>	<b>3</b>
<b>SECTION 3 VOLICO ENTERPRISE HOSTING SOLUTIONS' DESCRIPTION OF ITS CLOUD HOSTING, MANAGED SERVICES, DATA CENTER AND COLOCATION SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 1, 2018 TO JANUARY 31, 2019 .....</b>	<b>7</b>
OVERVIEW OF OPERATIONS .....	8
Company Background .....	8
Description of Services Provided .....	8
Principal Service Commitments and System Requirements .....	9
Components of the System .....	9
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING .....	16
Control Environment .....	16
Risk Assessment Process .....	17
Information and Communications Systems .....	18
Monitoring Controls .....	18
Changes to the System in the Last 12 Months .....	19
Incidents in the Last 12 Months .....	19
Criteria Not Applicable to the System .....	19
Subservice Organizations .....	19
COMPLEMENTARY USER ENTITY CONTROLS .....	19
TRUST SERVICES CATEGORIES .....	20
In-Scope Trust Services Criteria .....	20
<b>SECTION 4 TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS .....</b>	<b>21</b>
GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR.....	22
TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY .....	23
ADDITIONAL CRITERIA FOR AVAILABILITY .....	98

**SECTION 1**

**MANAGEMENT OF VOLICO ENTERPRISE HOSTING SOLUTIONS' ASSERTION  
REGARDING ITS SYSTEM THROUGHOUT THE PERIOD JULY 1, 2018 TO  
JANUARY 31, 2019**



**MANAGEMENT OF VOLICO ENTERPRISE HOSTING SOLUTIONS' ASSERTION REGARDING ITS SYSTEM THROUGHOUT THE PERIOD JULY 1, 2018 TO JANUARY 31, 2019**

June 3, 2019

We have prepared the accompanying description of VOLICO Enterprise Hosting Solutions' ('Volico' or 'the Company') Cloud Hosting, Managed Services, Data Center and Colocation Services System titled "VOLICO Enterprise Hosting Solutions' Description of Its Cloud Hosting, Managed Services, Data Center and Colocation Services System throughout the period July 1, 2018 to January 31, 2019", (description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Cloud Hosting, Managed Services, Data Center and Colocation Services that may be useful when assessing the risks arising from interactions with Volico's system, particularly information about system controls that Volico has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Volico's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Volico's controls.

We confirm, to the best of our knowledge and belief, that

- a. the description presents Volico's Cloud Hosting, Managed Services, Data Center and Colocation Services System that was designed and implemented throughout the period July 1, 2018 to January 31, 2019, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period July 1, 2018 to January 31, 2019, to provide reasonable assurance that Volico's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if user entities applied the complementary controls assumed in the design of Volico's controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period July 1, 2018 to January 31, 2019, to provide reasonable assurance that Volico's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of Volico's controls operated effectively throughout that period.

A handwritten signature in black ink, appearing to read "Gadi Hus", written over a horizontal line.

Gadi Hus  
Director of Operations/President  
VOLICO Enterprise Hosting Solutions

**SECTION 2**  
**INDEPENDENT SERVICE AUDITOR'S REPORT**

## INDEPENDENT SERVICE AUDITOR'S REPORT

To: VOLICO Enterprise Hosting Solutions

### *Scope*

We have examined Volico's accompanying description of its Cloud Hosting, Managed Services, Data Center and Colocation Services System titled "VOLICO Enterprise Hosting Solutions' Description of Its Cloud Hosting, Managed Services, Data Center and Colocation Services System throughout the period July 1, 2018 to January 31, 2019", (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2018 to January 31, 2019, to provide reasonable assurance that Volico's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Volico, to achieve Volico's service commitments and system requirements based on the applicable trust services criteria. The description presents Volico's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Volico's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

### *Service Organization's Responsibilities*

Volico is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Volico's service commitments and system requirements were achieved. Volico has provided its assertion titled "Management of VOLICO Enterprise Hosting Solutions' Assertion Regarding Its System Throughout the Period July 1, 2018 to January 31, 2019" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Volico is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

### *Service Auditor's Responsibilities*

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted 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, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

#### *Inherent Limitations*

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

#### *Description of Tests of Controls*

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4.

#### *Opinion*

In our opinion, in all material respects,

- a. the description presents Volico's Cloud Hosting, Managed Services, Data Center and Colocation Services System that was designed and implemented throughout the period July 1, 2018 to January 31, 2019, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period July 1, 2018 to January 31, 2019, to provide reasonable assurance that Volico's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the user entities applied the complementary controls assumed in the design of Volico's controls throughout the period.
- c. the controls stated in the description operated effectively throughout the period July 1, 2018 to January 31, 2019, to provide reasonable assurance that Volico's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of Volico's controls operated effectively throughout the period.

### *Restricted Use*

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Volico, user entities of Volico's Cloud Hosting, Managed Services, Data Center and Colocation Services during some or all of the period July 1, 2018 to January 31, 2019, business partners of Volico subject to risks arising from interactions with the Cloud Hosting, Managed Services, Data Center and Colocation Services, practitioners providing services to such user entities and business partners, prospective user entities and business partners, 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, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements 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 ASSURANCE

---

Tampa, Florida  
June 3, 2019

### **SECTION 3**

## **VOLICO ENTERPRISE HOSTING SOLUTIONS' DESCRIPTION OF ITS CLOUD HOSTING, MANAGED SERVICES, DATA CENTER AND COLOCATION SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 1, 2018 TO JANUARY 31, 2019**



## OVERVIEW OF OPERATIONS

### Company Background

Volico is an Enterprise-Class Data Center solutions provider founded in 2000, specializing in colocation, enterprise dedicated server hosting, disaster recovery, business continuity, backup services, private cloud computing, public cloud computing, managed firewall services, and CinC (Cloud in Cloud) IAAS computing.

With a vision of delivering a fully integrated trusted hosting environment, Volico's certified staff and high-profile product partners are able to provide enterprises with cost-effective and dependable hosting services. Whether as a primary service provider or business continuity/disaster recovery partner, Volico helps the businesses of today plan for tomorrow.

Volico currently operates multiple data centers servicing clients in Miami-Dade County, Broward County, and West-Palm Beach Counties of sunny South Florida. Volico's facilities are category 5 hurricane resistant, complete with gas-based inert fire suppression, 2N+X Smart-Grid redundant power infrastructure, and a 2N+X Smart-Grid redundant cooling infrastructure.

Additionally, the Volico Network Operations Center is manned 24x7x365 with knowledgeable, certified, and experienced network technicians that actively monitor infrastructure, connectivity, and application layer responsiveness. Any event immediately triggers a response from the Volico on-duty personnel.

Architected and engineered from the ground up with reliability and survivability in mind, Volico's 3rd Generation Data Center facilities utilize Smart-Grid infrastructure to maximize dependability and scalability of the facilities without sacrifices.

### Description of Services Provided

#### *Colocation*

Volico provides flexible, customizable, and cost-effective colocation solutions built to suit cages and suites of ¼, ½ and full private cabinets. From small businesses to large enterprise colocation, Volico is equipped to accommodate the needs of its customers.

#### *Dedicated Services*

Fully managed, dedicated servers offer scalability, security, uptime, and performance. Server hardware is built from high quality components and Volico's support technicians are certified experts in handling server equipment.

#### *Cloud Hosting*

Volico cloud services allow users to host their data remotely. From private VLANs to dedicated hardware clusters, customers can manage their data without hardware headaches.

#### *Managed Hosting*

Volico's managed hosting services and packages offer systemic maintenance and monitoring of client systems. Mission critical infrastructure is continually monitored in a maximum-security environment.

#### *Enterprise Hosting*

Volico delivers customized Enterprise Hosting Solutions to meet compliance needs and specific business. With years of experience in different application types and industries, Volico helps businesses and organizations move to the cloud with maximum service for the best value cost effective.

## Backup Services

Volico provides safe, flexible, and highly automated options for backup services with side-by-side comparisons. Customers can prevent a data disaster and allow Volico to automatically backup business/enterprise data.

## Principal Service Commitments and System Requirements

Volico provides a broad array of high-performance suites management solutions to meet clients' precise IT environment needs. Volico's managed services are backed and monitored by 24x7x365 onsite certified engineers' team, responsible with managing databases, security, and backups.

Volico guarantees 100% data center network uptime for its public Internet network, excluding scheduled maintenance. Notwithstanding the foregoing, users recognize that the Internet is comprised of thousands upon thousands of autonomous systems that are beyond the control of Volico. This SLA and the 100% Network Uptime Service Commitment cover the provision of access by Volico to the global internet "cloud".

Routing anomalies, asymmetries, inconsistencies and failures of the Internet outside of the control of Volico can and will occur, and such instances shall not be considered any failure of the 100% Network Uptime Service Commitment. Volico proactively monitors network uptime. The results of these monitoring systems shall provide the sole and exclusive determination of network uptime.

## Components of the System

### Infrastructure

Primary infrastructure used to provide Volico's Cloud Hosting, Managed Services, Data Center and Colocation Services System includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Servers	Client Specific (varies)	Hardware that supports the client's requirements. Could be HP, Dell, Supermicro or any other hardware they provide us.
Firewalls	Fortinet	Provide managed firewall services to clients.
Switches	Cisco	Connects client gear to Volico routes.
Routers	Cisco/Arista	Used for edge communication between Volico's facility and the outside network as well as internal communications.

### Software

Primary software used to provide Volico's Cloud Hosting, Managed Services, Data Center and Colocation Services System includes the following:

Primary Software		
Software	Operating System	Purpose
OS Free/Libre	GNU/Deb/Ubu/Centos/Freenas	Provide operating system base to clients requesting new servers.
OS Non-free	Windows Server family, Microsoft SQL	Provide operating system base to clients requesting new servers.

Primary Software		
Software	Operating System	Purpose
R1Soft	Linux/Win	Backup
Veeam	Linux/Win	Backup
Unitrends	Linux/Win	Backup

### *People*

Volico's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled and monitored. The organizational structure includes consideration of key areas of authority, responsibility and appropriate lines of reporting. Volico develops a dynamic organizational structure suited to its needs. The appropriateness of Volico's organizational structure depends, in part, on its size and the nature of its activities.

Volico's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are delegated and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, Volico includes policies and communications directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelated 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, responsibility and appropriate lines of escalation reporting to personnel.

### *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 Volico in delivering its Cloud Hosting, Managed Services, Data Center and Colocation 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
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, IDS alerts, or automated patching systems
- Incident reports documented via the ticketing systems

Customers interact with Volico employees directly through Volico's Internal management application. All data, reporting and logs are located in event log history of each customer. This includes device information, login details, etc.

Each output report is independent to each customer account and may be pulled from the customers dashboard.

Customers may utilize the management portal to view items such as invoices, services, power utilization, network utilization, support ticket requests, customer service requests, and even be able to manage remote power management of infrastructure.

### *Processes, Policies and Procedures*

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Volico's policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Volico team member.

## Physical Security

Management, technical support staff, and office administrators are responsible for Data Center access requirements. The management and monitoring of physical access to the Data Center is extremely important to Volico security and helps maintain information as well as employee safety.

Physical access to the Data Center shall be documented and managed. All Volico facilities must be physically protected relative to the criticality or importance of the function or purpose of the area managed.

Requests for access shall come from the applicable service department in the area where a new client or staff member of Volico will require access to the Data Center. Access to the Data Center will be granted only to personnel whose job responsibilities require access; or to documented clientele who have been certified by Volico administration. Electronic access control systems shall be used to manage access to the Data Center.

The process for granting card and/or key access resides with the Volico network operations center (NOC) Technical Support Department. They shall regularly review card and/or key access rights and remove access for individuals that no longer require access or persons who leave Volico. Access rights shall be based on an employee/client's role or function in the organization.

### Management Responsibilities

The NOC Technical Support Department or their designee shall ensure:

- Secure areas are protected by appropriate entry and controls for authorized personnel
- Procedures control and validate a staff member or client's access to the Data Center with the use of security personnel, identification badges, or electronic key cards
- Procedures exist that establish visitor controls including visitor sign-in logs and wearing of visitor badges for both entry and exit of the Volico
- Policies specify management's review of the list of individuals with physical access to the Data Center containing sensitive information (whether in paper or electronic forms)
- A complete inventory of critical assets is maintained with Volico ownership defined and documented
- Card access records and visitor logs for the Data Center are kept for review based upon the criticality of the information being protected and security necessity

### Key Access and Card Systems

The following policy applies to all Data Center access cards/keys:

- Employee and client access cards and/or keys must not be shared or loaned to others
- Access cards/keys shall not have identifying information and all cards/keys that are no longer required must be returned to Volico administration
- Lost or stolen cards/or keys must be reported immediately to Volico administration
- VOLICO administration shall remove card and/or key access rights of individuals that change roles or are separated from their relationship with Volico
- The NOC Technicians or their designee regularly reviews access records and visitor logs for the Data Center and is responsible for investigating any unusual events or incidents related to physical facility access

### Visitor and Guest Access

The following policy and procedures apply to identification and authorization of visitors and guests to Volico:

- Any Volico facility that allows access to visitors shall document visitor access with a sign in/out log physically or electronically
- A visitor log shall be used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where sensitive information is stored or transmitted

- The visitor log shall document the visitor's name, the company represented, and the on-site personnel authorizing physical access on the log
- The visitor log shall be retained for a minimum of three months, unless otherwise restricted by rule, regulation, statute, or Volico audit control
- Visitors shall be identified and given a badge or other identification that expires and that visibly distinguishes the visitors from on-site personnel
- Visitors shall surrender the badge or identification before leaving the facility or at the date of expiration
- Visitors shall be authorized before entering, and escorted at all times within, areas where sensitive information is processed or maintained
- Visitors must be escorted in card access controlled areas of the facility

#### Confidential Area Access

The following policy and procedure pertain to access to confidential Volico areas:

- All areas containing sensitive information shall be physically restricted
- All individuals in these areas must wear an identification badge on their person so that both the picture and information on the badge are clearly visible to Volico personnel
- Restricted IT areas such as data centers, computer rooms, telephone closets, network router and hub rooms, voice-mail system rooms, and similar areas containing IT resources shall be restricted based upon functional business need
- Physical access to records containing sensitive information, and storage of such records and data in locked facilities, storage areas, or containers shall be restricted
- Sensitive IT resources located in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access to sensitive information
- Appropriate facility entry controls shall limit and monitor physical access to information systems
- Video cameras and/or access control mechanisms shall monitor individual physical access to sensitive areas and this data shall be stored for at least three months, unless otherwise restricted by rule, regulation, statute, or law

Volico NOC Technician Staff Shall:

- Implement physical and/or logical controls to restrict access to publicly accessible data jacks (for example, data jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized)
- Ensure visitors are escorted at all times in areas with sensitive information
- Areas accessible to visitors should not have enabled data jacks unless network access is provided to a secure guest network only
- Restrict physical access to wireless access points, gateways, handheld devices, networking, communications hardware, and telecommunications lines
- Control physical and logical access to diagnostic and configuration ports
- Receive prior authorization before disposing, relocating, or transferring hardware, software, or data to any offsite premises

#### Physical Site Access

On-site physical access to sensitive or confidential areas for shall be controlled though a combination of the following mechanisms:

- Security based on individual job function or role
- Revocation of all facility access immediately upon termination and collection of keys, access/smart cards, and/or any other asset used to enter Volico facilities

Policies and procedures shall be established to ensure the secure use, asset management, and secure repurposing and disposal of equipment maintained and used outside the organization's premises.

## Contractor Requirements

External contractors shall comply with applicable laws and regulations regarding security and background checks when working in Volico facilities. For unclassified personnel, an appropriately cleared and technically knowledgeable staff member shall escort the individual to the area where facility maintenance is being performed and ensure that appropriate security procedures are followed:

- Any system access, initiation or termination shall be performed by the escort
- Keystroke monitoring shall be performed during access to the system
- Prior to maintenance, the information system is completely cleared, and all non-volatile data storage media shall be removed or physically disconnected and secured
- Maintenance personnel must not have visual or electronic access to any sensitive or confidential information contained on the system they are servicing
- Devices that display or output sensitive information in human-readable form shall be positioned to prevent unauthorized individuals from reading the information
- All personnel granted unescorted access to the physical area containing the information system shall have an appropriate security clearance

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of normal Volico operations. Examples of acceptable controls and procedures include:

- Visitor logs
- Access control procedures and processes
- Operational key-card access and premise control systems
- Operational video surveillance systems and demonstrated archival retrieval

## Logical Access

Volico uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, Volico implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing reviews of access by role.

Employees and approved vendor personnel sign on to the Volico network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from outside the Volico network are required to use a token-based two-factor authentication system. Employees are issued tokens upon employment and must return the token during their exit interview. Vendor personnel are not permitted to access the system from outside the Volico network.

Upon hire, employees are assigned to a position in the HR management system. Two days prior to the employees' start date, the HR management system creates a report of employee user IDs to be created and access to be granted. The report is used by the security help desk to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for each role are reviewed by a working group composed of security help desk, data center, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the CTO. As part of this process, the CTO reviews access by privileged roles and requests modifications based on this review.

The HR system generates a list of terminated employees on a daily basis. This daily report is used by the security help desk to delete employee access. On an annual basis, HR runs a list of active employees. The security help desk uses this list to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

On an annual basis, managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the security help desk for processing. The security help desk manager identifies any records not returned within two weeks and follows up with the manager. As part of this process, the CTO reviews employees with access to privileged roles and requests modifications through the event management system.

#### Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Backup infrastructure and on-site backup tape media are physically secured in locked cabinets and/or caged environments within the third-party data centers. The backup infrastructure resides on private networks logically secured from other networks.

Contracted customer off-site tape rotations are logged and maintained within an enterprise ticket management system. A third-party provider that specializes in off-site tape rotation has been contracted to perform off-site tape rotation services for clients that select this as part of the backup service. The ability to recall backup media from the third-party off-site storage facility is restricted to authorized operations personnel.

#### Computer Operations - Availability

The Volico Security Incident Response Plan applies to all networks, systems, and data as well as members of the organization including employees and contractors as well as vendors that access the networks, systems, and data.

Members of the organization who may be called upon to lead or participate as part of the Security Incident Response Team must familiarize themselves with this plan and be prepared to collaborate with the goal of minimizing adverse impact to the organization.

The Incident Handler monitors for incidents in Volico's internal management application and other monitoring tools and acknowledges that when a high or critical security incident is underway, responsibility for managing the incident is entrusted to the Incident Handler or their delegate.

The Incident Handler or a delegate is expected to handle the incident in a way that mitigates further exposure of the organization. The incident will be handled according to process including identification, containment, eradication, recovery, and lessons learned.

### Change Control

Volico Data Centers maintains a change management policy to track all changes made to the core infrastructure, made available through an internal wiki. A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Volico Data Centers utilize many built-in change control systems available from tools like GitLab and its Internal management application (ticketing system). The change management Plan documents and tracks the necessary information required to effectively manage project change from project inception to delivery. The Change Management Plan is created during the planning phase of each project. Its intended audience is the project manager, project team, project sponsor and any senior leaders whose support is needed to carry out the plan. Volico's ticketing system tracks every change in real time for each customer. Special projects utilize Volico's change management template and adheres to the project for the template.

### Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees. Volico monitors the internal firewall, critical systems and critical production applications and act/perform as needed on the alerts. All major enhancements, upgrades, conversions, and related changes associated with these systems or applications are preceded by a risk assessment or penetration test prior to deployment.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place. The data center operates a 2N+X Smart-Grid redundant power infrastructure, and a 2N+X Smart-Grid redundant cooling infrastructure for redundancy.

All systems being implemented or constructed are assessed for vulnerability by a project-oriented team during the preliminary design phase and throughout its operation life. Penetration testing is performed on core applications and services as they are deployed or being tested for deployment.

Authorized employees may access the system through from the Internet through the use of leading VPN technology, managed by the network and security team.

### *Boundaries of the System*

The scope of this report includes the Cloud Hosting, Managed Services, Data Center and Colocation Services System performed in the Deerfield, Florida facilities.



## **RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING**

### **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 Volico's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Volico'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*

Volico'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.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

#### *Management's Philosophy and Operating Style*

Volico'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 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*

Volico'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.

Volico'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.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility
- Organizational charts are communicated to employees and updated as needed

### *Human Resources Policies and Practices*

Volico'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. Volico'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 Process**

Volico's risk assessment process identifies and manages risks that could potentially affect Volico'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. Volico 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 Volico, 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

Volico has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. 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. Volico attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

#### *Integration with Risk Assessment*

The environment in which the system operates; the commitments, agreements, and responsibilities of Volico's Cloud Hosting, Managed Services, Data Center and Colocation Services System; as well as the nature of the components of the system result in risks that the criteria will not be met. Volico 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, Volico's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

#### **Information and Communications Systems**

Information and communication is an integral component of Volico'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 Volico, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Volico personnel via e-mail messages.

Specific information systems used to support Volico's Cloud Hosting, Managed Services, Data Center and Colocation Services System are described in the Description of Services section above.

#### **Monitoring Controls**

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Volico'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*

Volico'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 Volico'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 Volico'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.

### **Changes to the System in the Last 12 Months**

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

### **Incidents in the Last 12 Months**

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

### **Criteria Not Applicable to the System**

All Common and Availability criterion was applicable to the Volico Cloud Hosting, Managed Services, Data Center and Colocation Services System.

### **Subservice Organizations**

No subservice organizations were included in the scope of this assessment.

## **COMPLEMENTARY USER ENTITY CONTROLS**

Volico'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 Criteria related to Volico's services to be solely achieved by Volico control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Volico's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria 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 Volico.
2. User entities are responsible for notifying Volico of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Volico services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Volico services.

6. User entities are responsible for providing Volico with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Volico of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

## TRUST SERVICES CATEGORIES

### In-Scope Trust Services Criteria

#### Common Criteria (to the Security and Availability Categories)

Security refers to the protection of

- i. information during its collection or creation, use, processing, transmission, and storage and
- ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

#### Availability

Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

#### *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 Volico's description of the system. Any applicable trust services criteria that are not addressed by control activities at Volico are described within Section 4.

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.

**SECTION 4**

**TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND  
TESTS OF CONTROLS**

# GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of Volico was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Volico and did not encompass all aspects of Volico'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 was 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 criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization
- Determine whether the criteria are relevant to the user entity's assertions
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria

**Control Activities Specified by the Service Organization**

<b>TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</b>				
<b>Control Environment</b>				
<b>CC1.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	<p>Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.</p> <p>An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.</p> <p>Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.</p> <p>Upon hire, personnel are required to complete a background check.</p> <p>Sanction policies which include probation, suspension and termination are in place for employee misconduct.</p>	<p>Inspected the employee handbook to determine that core values were communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.</p> <p>Inspected the employee handbook to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.</p> <p>Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.</p> <p>Inspected the completed background check form for a sample of new hires to determine that upon hire, personnel were required to complete a background check.</p> <p>Inspected the employee handbook to determine that sanction policies which include probation, suspension and termination were in place for employee misconduct.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Control Environment**

<b>CC1.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	<p>Users of the system are directed on how to report unethical behavior in a confidential manner.</p> <p>Executive management roles and responsibilities are documented and reviewed annually.</p> <p>Executive management maintains independence from those that operate the key controls within the environment.</p> <p>Executive management meets at least annually with operational management to assess the effectiveness and performance of internal controls within the environment.</p>	<p>Inspected the employee handbook and the third-party and customer contract templates to determine that users of the system were directed on how to report unethical behavior in a confidential manner.</p> <p>Inspected the written executive job descriptions to determine that executive management roles and responsibilities were documented and reviewed annually.</p> <p>Inspected the organizational chart to determine that executive management-maintained independence from those that operated the key controls within the environment.</p> <p>Inspected the executive meeting schedule to determine that executive management met at least annually with operational management to assess the effectiveness and performance of internal controls within the environment.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Control Environment**

<b>CC1.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.  A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.  Executive management reviews the organization chart annually and makes updates to the organizational structure and lines of reporting, when necessary.  Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the internal controls matrix to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls implemented within the environment.  Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.  Inspected the revision date of the organizational chart to determine that executive management reviewed the organization chart annually and made updates to the organizational structure and lines of reporting, when necessary.  Inspected the written job description for a sample of roles to determine that executive management reviewed job descriptions annually and made updates, if necessary.	No exceptions noted.  No exceptions noted.  No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Control Environment**

<b>CC1.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	<p>Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.</p> <p>Executive management has established proper segregations of duties for key job functions and roles within the organization.</p> <p>Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.</p> <p>The entity evaluates the competencies and experience of candidates prior to hiring.</p>	<p>Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook which required adherence to the personnel's job role and responsibilities.</p> <p>Inspected the organizational chart and the written job description for a sample of executive roles to determine that executive management had established proper segregations of duties for key job functions and roles within the organization.</p> <p>Inspected the employee handbook to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.</p> <p>Inspected the retained new hire evaluation materials to determine that the entity evaluated the competencies and experience of candidates prior to hiring.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Control Environment**

<b>CC1.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>New hire candidates' abilities to meet job requirements are evaluated as part of the hiring process.</p> <p>New hire performance is evaluated after a 90-day period.</p> <p>Current employees are required to complete information security and awareness training on an annual basis.</p> <p>Executive management develops information security training materials to train personnel.</p>	<p>Inspected the retained new hire evaluation materials to determine that new hire candidates' abilities to meet job requirements were evaluated as part of the hiring process.</p> <p>Inspected the new hire evaluations for a sample of new hires to determine that new hire performance was evaluated after a 90-day period.</p> <p>Inquired of the President regarding information security training to determine that current employees were required to complete information security and awareness training on an annual basis.</p> <p>Inspected the information security awareness policy and the information security training completion forms for a sample of current employees to determine that current employees were required to complete information security and awareness training on an annual basis.</p> <p>Inspected the security awareness training materials to determine that executive management developed information security training materials to train personnel.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Control Environment**

<b>CC1.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	<p>A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.</p> <p>Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.</p> <p>Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.</p> <p>Sanction policies which include probation, suspension and termination are in place for employee misconduct.</p>	<p>Prior to employment, personnel are required to complete a background check.</p> <p>Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.</p> <p>Inspected the completed background checks for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.</p> <p>Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.</p> <p>Inspected a signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook which required adherence to the personnel's job role and responsibilities.</p> <p>Inspected the employee handbook and information security training policy to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.</p> <p>Inspected the employee handbook to determine that sanction policies which include probation, suspension and termination were in place for employee misconduct.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Information and Communication**

<b>CC2.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.	Inspected the information security policy and the company intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.	No exceptions noted.
		Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the data flow diagram to determine that data flow diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
		Data entered into the system, processed by the system, and output from the system is protected from unauthorized access.	Inspected the Intrusion Detection System (IDS) configurations and the encryption configurations to determine that data entered into the system, processed by the system, and output from the system was protected from unauthorized access.	No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's website.	Inspected the job descriptions on the company intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's share drive.	No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Information and Communication**

<b>CC2.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>The entity's employee handbook is reviewed on an annual basis.</p> <p>The entity's policies and procedures are made available to employees through the entity's intranet.</p> <p>Upon hire, employees are required to read and acknowledge the entity's information security policies and procedures and complete information security and awareness training.</p> <p>Employees are required to sign an acknowledgement whenever significant changes are made to the employee handbook.</p>	<p>Inspected the employee handbook to determine that the entity's employee handbook was reviewed on an annual basis.</p> <p>Inspected the entity intranet to determine that the entity's policies and procedures were made available to employees through the entity's intranet.</p> <p>Inspected the signed employee handbook and information security training completion for a sample of new hires to determine that upon hire, employees were required to read and acknowledge the entity's information security policies and procedures and complete information security and awareness training.</p> <p>Inquired of the President regarding handbook revision procedures to determine that employees were required to sign an acknowledgement whenever significant changes were made to the employee handbook.</p> <p>Inspected the employee handbook to determine that employees were required to sign an acknowledgement whenever significant changes were made to the employee handbook.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Information and Communication**

<b>CC2.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Current employees are required to complete information security and awareness training on an annual basis.</p> <p>Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.</p>	<p>Inspected the handbook revision acknowledgement for a sample of current employees to determine that employees were required to sign an acknowledgement whenever significant changes were made to the employee handbook.</p> <p>Inquired of the President regarding information security training to determine that current employees were required to complete information security and awareness training on an annual basis.</p> <p>Inspected the information security awareness policy and the information security training completion forms for a sample of current employees to determine that current employees were required to complete information security and awareness training on an annual basis.</p> <p>Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.</p>	<p>Testing of the control activity disclosed that there were no significant revisions to the employee handbook during the review period.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Information and Communication**

<b>CC2.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.</p>	<p>Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook which required adherence to the personnel's job role and responsibilities.</p>	<p>No exceptions noted.</p>
		<p>Users of the system are directed on how to report unethical behavior in a confidential manner.</p>	<p>Inspected the employee handbook and the third-party and customer contract templates to determine that users of the system were directed on how to report unethical behavior in a confidential manner.</p>	<p>No exceptions noted.</p>
		<p>Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's intranet.</p>	<p>Inspected the incident response policy and the company intranet to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and made available to employees through the entity's intranet.</p>	<p>No exceptions noted.</p>
		<p>The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's website.</p>	<p>Inspected the entity's website to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's website.</p>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Information and Communication**

<b>CC2.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	<p>The entity's third-party agreement delineates the boundaries of the system and describes relevant system components.</p> <p>The entity adheres to third-party agreements that delineate system commitments and requirements of third parties.</p> <p>The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system.</p>	<p>Inspected the third-party and customer contract templates to determine that the entity's third-party agreement delineated the boundaries of the system and described relevant system components.</p> <p>Inspected the third-party agreement for a sample of vendors to determine that the entity adhered to third-party agreements that delineated system commitments and requirements of third-parties.</p> <p>Inquired of the President regarding vendor system access to determine that the information security policies and procedures that communicated the system commitments and requirements of external users were provided to external users prior to allowing them access to the system.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Information and Communication**

<b>CC2.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third parties.</p> <p>Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.</p> <p>Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place with existing third-parties and shared with external parties.</p>	<p>Inspected the third-party agreement for a sample of vendors to determine that the entity's third-party agreement outlined and communicated the terms, conditions and responsibilities of third-parties.</p> <p>Inspected the contract for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.</p> <p>Inspected the third-party contracts in place and the entity's knowledgebase and available policies to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place with existing third-parties and shared with external parties.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Information and Communication**

<b>CC2.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Employees, third parties and customers are directed on how to report unethical behavior in a confidential manner. There is a support section and live chat featured on the entity's website to direct external users in reporting incidents.</p>	<p>Inspected the employee handbook, the incident response policy, the entity's website and the third-party service agreements in place to determine that employees, third parties and customers were directed on how to report unethical behavior in a confidential manner, and there was a support section and live chat featured on the entity's website to direct external users in reporting incidents.</p>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Assessment**

<b>CC3.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	<p>The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.</p> <p>Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.</p> <p>Executive management has established key performance indicators for operational effectiveness.</p> <p>Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.</p>	<p>Inspected the entity's strategy document to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.</p> <p>Inquired of the President regarding risk assessment to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.</p> <p>Inspected the risk assessment policy to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.</p> <p>Inspected the key performance indicators to determine that executive management had established key performance indicators for operational effectiveness.</p> <p>Inquired of the President regarding compliance monitoring to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Assessment**

<b>CC3.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	<p>The entity's internal controls framework is based on the COSO framework.</p> <p>Documented policies and procedures are in place to guide personnel when performing a risk assessment.</p> <p>Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks, and defining specified risk tolerances.</p>	<p>Inspected the written executive job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.</p> <p>Inspected the attestation report to determine that the entity's internal controls framework was based on the COSO framework.</p> <p>Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.</p> <p>Inquired of the President regarding risk assessment to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks, and defining specified risk tolerances.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Assessment**

<b>CC3.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.</p>	<p>Inspected the risk assessment policy to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks, and defining specified risk tolerances.</p> <p>Inspected the completed risk assessment to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks, and defining specified risk tolerances.</p> <p>Inquired of the President regarding the risk assessment process to determine that a formal risk assessment was performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Assessment**

<b>CC3.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
			<p>Inspected the risk assessment policy to determine that a formal risk assessment was performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.</p> <p>Inspected the completed risk assessment to determine that a formal risk assessment was performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Assessment**

<b>CC3.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>The entity's risk assessment process includes:</p> <ul style="list-style-type: none"> <li>• Identifying the relevant information assets that are critical to business operations</li> <li>• Prioritizing the criticality of those relevant information assets</li> <li>• Identifying and assessing the impact of the threats to those information assets</li> <li>• Identifying and assessing the impact of the vulnerabilities associated with the identified threats</li> <li>• Assessing the likelihood of identified threats and vulnerabilities</li> <li>• Determining the risks associated with the information assets</li> <li>• Addressing the associated risks identified for each identified vulnerability</li> </ul>	<p>Inquired of the President regarding the risk assessment methodology to determine that the entity's risk assessment process included:</p> <ul style="list-style-type: none"> <li>• Identifying the relevant information assets that are critical to business operations</li> <li>• Prioritizing the criticality of those relevant information assets</li> <li>• Identifying and assessing the impact of the threats to those information assets</li> <li>• Identifying and assessing the impact of the vulnerabilities associated with the identified threats</li> <li>• Assessing the likelihood of identified threats and vulnerabilities</li> <li>• Determining the risks associated with the information assets</li> <li>• Addressing the associated risks identified for each identified vulnerability</li> </ul>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Assessment**

<b>CC3.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
			<p>Inspected the risk assessment policy to determine that the entity's risk assessment process included:</p> <ul style="list-style-type: none"> <li>• Identifying the relevant information assets that are critical to business operations</li> <li>• Prioritizing the criticality of those relevant information assets</li> <li>• Identifying and assessing the impact of the threats to those information assets</li> <li>• Identifying and assessing the impact of the vulnerabilities associated with the identified threats</li> <li>• Assessing the likelihood of identified threats and vulnerabilities</li> <li>• Determining the risks associated with the information assets</li> <li>• Addressing the associated risks identified for each identified vulnerability</li> </ul>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Assessment**

<b>CC3.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Identified risks are rated using a risk evaluation process and ratings are approved by management.</p>	<p>Inspected the completed risk assessment to determine that the entity's risk assessment process included:</p> <ul style="list-style-type: none"> <li>• Identifying the relevant information assets that are critical to business operations</li> <li>• Prioritizing the criticality of those relevant information assets</li> <li>• Identifying and assessing the impact of the threats to those information assets</li> <li>• Identifying and assessing the impact of the vulnerabilities associated with the identified threats</li> <li>• Assessing the likelihood of identified threats and vulnerabilities</li> <li>• Determining the risks associated with the information assets</li> <li>• Addressing the associated risks identified for each identified vulnerability</li> </ul> <p>Inquired of the President regarding risk identification to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Assessment**

<b>CC3.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Management develops risk mitigation strategies to address risks identified during the risk assessment process.</p>	<p>Inspected the risk assessment policy to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.</p> <p>Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.</p> <p>Inspected the risk assessment policy to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.</p>	<p>No exceptions noted.</p>
		<p>For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.</p>	<p>Inquired of the President regarding risk remediation to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.</p>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Assessment**

<b>CC3.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud (e.g. fraudulent reporting, loss of assets, unauthorized system access, overriding controls) that could impact their business and operations.	<p>Inspected the risk assessment policy to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.</p> <p>Inspected the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.</p> <p>Inspected the fraud assessment report to determine that on an annual basis, management identified and assessed the types of fraud (e.g. fraudulent reporting, loss of assets, unauthorized system access, overriding controls) that could impact their business and operations.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Assessment**

<b>CC3.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	<p>Inquired of the President regarding fraud assessment to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.</p> <p>Inspected the risk assessment report to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.</p> <p>Inquired of the President regarding risk adaptation to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.</p> <p>Inspected the risk assessment policy to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Assessment**

<b>CC3.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Changes to the entity's systems, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.</p>	<p>Inspected the completed risk assessment to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.</p> <p>Inquired of the President regarding business risk adaptation to determine that changes to the entity's systems, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.</p> <p>Inspected the risk assessment policy to determine that changes to the entity's systems, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.</p> <p>Inspected the completed risk assessment to determine that changes to the entity's systems, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Monitoring Activities**

<b>CC4.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC4.1	<p>COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.</p>	<p>Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.</p> <p>Management reviews policies, procedures and other control documents for accuracy and applicability, and makes revisions when significant changes are made.</p> <p>On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.</p>	<p>Inspected the monitoring system dashboard to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.</p> <p>Inquired of the President regarding policy revision to determine that management reviewed policies, procedures and other control documents for accuracy and applicability, and made revisions when significant changes were made.</p> <p>Inspected the employee handbook to determine that management reviewed policies, procedures and other control documents for accuracy and applicability, and made revisions when significant changes were made.</p> <p>Inquired of the President regarding internal control evaluation to determine that on an annual basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Monitoring Activities**

<b>CC4.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Key systems, tools, and applications are reviewed internally for compliance against documented policies and procedures by operational management annually using a compliance monitoring tool.</p> <p>Control self-assessments that include, but are not limited to logical access reviews, including network, operating system, data storage and VPN, and backup restoration tests are performed on at least an annual basis.</p>	<p>Inspected the management meeting schedule to determine that on an annual basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.</p> <p>Inspected the internal compliance assessment and the monitoring tool dashboard to determine that key systems, tools, and applications were reviewed internally for compliance against documented policies and procedures by operational management annually using a compliance monitoring tool.</p> <p>Inquired of the President regarding control evaluation to determine that control self-assessments that included, but were not limited to logical access reviews, including network, operating system, data storage and VPN, and backup restoration tests were performed on at least an annual basis.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Monitoring Activities**

<b>CC4.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Vulnerability scans are performed annually on the environment to identify control gaps and vulnerabilities.</p> <p>A third-party collaborates with the entity to produce an assessment of the controls environment annually to assess the effectiveness of controls within the environment.</p> <p>Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.</p>	<p>Inspected the completed backup restoration test and the completed logical access review to determine that control self-assessments that included, but were not limited to logical access reviews, including network, operating system, data storage and VPN, and backup restoration tests were performed on at least an annual basis.</p> <p>Inspected the completed vulnerability scan to determine that vulnerability scans were performed annually on the environment to identify control gaps and vulnerabilities.</p> <p>Inspected the completed attestation report to determine that a third-party collaborated with the entity to produce an assessment of the controls environment annually to assess the effectiveness of controls within the environment.</p> <p>Inspected the third-party attestation report to determine that management obtained and reviewed attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Monitoring Activities**

<b>CC4.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	Inquired of the President regarding system vulnerability awareness to determine that senior management was made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.  Inspected an example automated system security response and automated helpdesk ticket to determine that senior management was made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	No exceptions noted.  No exceptions noted.
		Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions.	Inquired of the President regarding remedial procedures to determine that vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Monitoring Activities**

<b>CC4.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner.</p>	<p>Inspected the incident response policy to determine that vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions.</p> <p>Inspected an example automated system security response and automated system anomaly ticket to determine that vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Control Activities**

<b>CC5.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations (e.g. risk assessments, vulnerability scans) performed.  Performance of the internal controls implemented within the environment are assigned to appropriate personnel based on roles and responsibilities.	Inquired of the President regarding the risk assessment to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations (e.g. risk assessments, vulnerability scans) performed.  Inspected the internal controls matrix to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations (e.g. risk assessments, vulnerability scans) performed.	No exceptions noted.  No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the company policies and the internal controls matrix to determine that management had documented the relevant controls in place for each key business or operational process.	No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Control Activities**

<b>CC5.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the company policies and the internal controls matrix to determine that management had incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the business continuity and disaster recovery test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive.	Inspected the policies and procedures on the entity's intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive.	No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Control Activities**

<b>CC5.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	<p>The internal controls implemented around the entity's technology infrastructure include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Restricting access rights to authorized users</li> <li>• Limiting services to what is required for business operations</li> <li>• Authentication of access</li> <li>• Protecting the entity's assets from external threats</li> </ul> <p>Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive.</p>	<p>Inspected the risk assessment policy and the internal controls matrix to determine that management had established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.</p> <p>Inspected the entity's security policies and the internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to:</p> <ul style="list-style-type: none"> <li>• Restricting access rights to authorized users</li> <li>• Limiting services to what is required for business operations</li> <li>• Authentication of access</li> <li>• Protecting the entity's assets from external threats</li> </ul> <p>Inspected the policies and procedures on the entity's intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Control Activities**

<b>CC5.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Management has implemented controls that are built into the organizational and information security policies and procedures.</p> <p>Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.</p>	<p>Inspected the entity's security policies and the internal controls matrix to determine that management has implemented controls that were built into the organizational and information security policies and procedures.</p> <p>Inspected the internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>



**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	An inventory of system assets and components is maintained to classify and manage the information assets.  Privileged access to sensitive resources including network, operating system, data storage and VPN is restricted to authorized personnel.	Inspected the inventory listing of system assets to determine that an inventory of system assets and components was maintained to classify and manage the information assets.  Inquired of the President regarding network administrative access to determine that privileged access to sensitive resources including network, operating system, data storage and VPN was restricted to authorized personnel.	No exceptions noted.  No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the entity's security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
	<b>Network</b>	<p>Network user access is restricted via role-based security privileges defined within the access control system.</p> <p>Network administrative access is restricted to user accounts accessible by authorized personnel.</p>	<p>Inquired of the President regarding network user access to determine that network user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inspected the network user listing to determine that network user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inquired of the President regarding network administrative access to determine that network administrative access was restricted to user accounts accessible by authorized personnel.</p> <p>Inspected the network admin listing to determine that network administrative access was restricted to user accounts accessible by authorized personnel.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
		<p>Networks are configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> <li>• Password history</li> <li>• Password length</li> <li>• Password age</li> </ul>	<p>Inspected the network password configurations to determine that networks were configured to enforce password requirements that included:</p> <ul style="list-style-type: none"> <li>• Password history</li> <li>• Password length</li> <li>• Password age</li> </ul>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Network audit logging settings are in place that include:</p> <ul style="list-style-type: none"> <li>• Account logon events</li> <li>• Account management</li> <li>• Logon events</li> <li>• System events</li> </ul> <p>Network audit logs are maintained and monitored.</p>	<p>Inspected an example automated audit log extract to determine that network audit logging settings were in place that included:</p> <ul style="list-style-type: none"> <li>• Account logon events</li> <li>• Account management</li> <li>• Logon events</li> <li>• System events</li> </ul> <p>Inquired of the President regarding log reviewal to determine that network audit logs were maintained and monitored.</p> <p>Inspected an example automated audit log extract to determine that network audit logs were maintained and reviewed, when necessary.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
	<b>Operating System</b>			
		<p>Operating system user access is restricted via role-based security privileges defined within the access control system.</p>	<p>Inquired of the President regarding operating system access to determine that operating system user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inspected the user listing for the in-scope operating system to determine that operating system user access was restricted via role-based security privileges defined within the access control system.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Operating system administrative access is restricted to user accounts accessible by authorized personnel.</p>	<p>Inquired of the President regarding operating system administrative access to determine that operating system administrative access was restricted to user accounts accessible by authorized personnel.</p>	<p>No exceptions noted.</p>
		<p>Operating system users are authenticated via individually-assigned user accounts and passwords.</p>	<p>Inspected the administrator listing for the in-scope the operating system to determine that operating system administrative access was restricted to user accounts accessible by authorized personnel.</p>	<p>No exceptions noted.</p>
			<p>Inquired of the President regarding operating system authentication to determine that operating system users were authenticated via individually-assigned user accounts and passwords.</p>	<p>Observed the operating system authentication process to determine that operating system users were authenticated via individually-assigned user accounts and passwords.</p>
				<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Operating system audit logging settings are in place that include:</p> <ul style="list-style-type: none"> <li>• Account logon events</li> <li>• Account management</li> <li>• Logon events</li> <li>• System events</li> </ul> <p>Operating system audit logs are maintained and monitored.</p>	<p>Inspected an example automated audit log extract to determine that operating system audit logging settings were in place that included:</p> <ul style="list-style-type: none"> <li>• Account logon events</li> <li>• Account management</li> <li>• Logon events</li> <li>• System events</li> </ul> <p>Inquired of the President regarding log reviewal to determine that operating system audit logs were maintained and monitored.</p> <p>Inspected an example automated audit log extract to determine that operating system audit logs were maintained and reviewed, when necessary.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
	<b>Data Storage</b>			
		<p>Data storage system user access is restricted via role-based security privileges defined within the access control system.</p>	<p>Inquired of the President regarding data storage tool access to determine that data storage system user access was restricted via role-based security privileges defined within the access control system.</p>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Data storage administrative access is restricted to authorized personnel.</p>	<p>Inquired of the President regarding data storage administrative access to determine that data storage administrative access was restricted to authorized personnel.</p>	<p>No exceptions noted.</p>
		<p>Data storage systems are configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> <li>• Password history</li> <li>• Password length</li> <li>• Password age</li> </ul>	<p>Inspected the user listing for the in-scope data storage system infrastructure to determine that data storage tool user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inquired of the President regarding data storage administrative access to determine that data storage administrative access was restricted to authorized personnel.</p> <p>Inspected the administrator listing for the in-scope data storage infrastructure to determine that data storage administrative access was restricted to authorized personnel.</p> <p>Inspected the password configurations for the in-scope data storage infrastructure to determine that data storage systems were configured to enforce password requirements that included:</p> <ul style="list-style-type: none"> <li>• Password history</li> <li>• Password length</li> <li>• Password age</li> </ul>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Data storage users are authenticated via individually-assigned user accounts and passwords.</p> <p>Data storage audit logging settings are in place that include:</p> <ul style="list-style-type: none"> <li>• Account logon events</li> <li>• Account management</li> <li>• Logon events</li> <li>• System events</li> </ul> <p>Data storage audit logs are maintained and monitored.</p>	<p>Inquired of the President regarding data storage access to determine that data storage users were authenticated via individually-assigned user accounts and passwords.</p> <p>Inspected the data storage password configurations to determine that data storage users were authenticated via individually-assigned user accounts and passwords.</p> <p>Inspected an example automated audit log extract for the in-scope data storage infrastructure to determine that data storage audit logging settings were in place that included:</p> <ul style="list-style-type: none"> <li>• Account logon events</li> <li>• Account management</li> <li>• Logon events</li> <li>• System events</li> </ul> <p>Inquired of the President regarding log reviewal to determine that data storage audit logs were maintained and monitored.</p> <p>Inspected an example automated audit log extract for the in-scope data storage infrastructure to determine that data storage audit logs were maintained and reviewed, when necessary.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
	<b>Remote Access</b>	<p>Virtual Private Network (VPN) user access is restricted via role-based security privileges defined within the access control system.</p> <p>The ability to administer VPN access is restricted to user accounts accessible by authorized personnel.</p> <p>VPN users are authenticated via individually-assigned user accounts and passwords.</p>	<p>Inquired of the President regarding remote access to determine that VPN user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inquired of the President regarding remote administrative access to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel.</p> <p>Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel.</p> <p>Inquired of the President regarding VPN authentication to determine that VPN users were authenticated via individually-assigned user accounts and passwords.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC6.2	<p>Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.</p>	<p>Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.</p> <p>Logical access to systems is granted to employees as a component of the hiring process.</p>	<p>Observed an authorized user login to the remote access system to determine that VPN users were authenticated via individually-assigned user accounts and passwords.</p> <p>Inspected the VPN authentication configurations to determine that VPN users were authenticated via individually-assigned user accounts and passwords.</p> <p>Inspected the entity's security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.</p> <p>Inquired of the President regarding new hire access to determine that logical access to systems was granted to employees as a component of the hiring process.</p> <p>Inspected the access request ticket for a sample of new hires and the written new hire process to determine that logical access to systems was granted to employees as a component of the hiring process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Logical access to systems is revoked as a component of the termination process.</p>	<p>Inquired of the President regarding access revocation to determine that logical access to systems was revoked as a component of the termination process.</p> <p>Inspected the employee handbook and sanction policies to determine that logical access to systems was revoked as a component of the termination process.</p> <p>Inspected the system and user access listing and termination request and checklist for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process.</p> <p>Inspected the completed access review performed by management to determine that control self-assessments that included logical access reviews were performed on at least an annual basis.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no employees were terminated during the review period.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.  Logical access to systems is granted to employees as a component of the hiring process.	Inspected the entity's security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.  Inquired of the President regarding new hire access to determine that logical access to systems was granted to employees as a component of the hiring process.  Inspected the access request ticket for a sample of new hires and the written new hire process to determine that logical access to systems was granted to employees as a component of the hiring process.	No exceptions noted.  No exceptions noted.  No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the President regarding access revocation to determine that logical access to systems was revoked as a component of the termination process.  Inspected the employee handbook and sanction policies to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	<p>Control self-assessments that include logical access reviews are performed on at least an annual basis.</p> <p>Policies and procedures are in place to guide personnel in physical security activities.</p> <p>Physical access to systems is approved and granted to an employee as a component of the hiring process.</p> <p>A manned reception desk is in place to monitor and control access to the entrance of the office facility during standard business hours.</p>	<p>Inspected the system and user access listing and termination request and checklist for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process.</p> <p>Inspected the completed access review performed by management to determine that control self-assessments that included logical access reviews were performed on at least an annual basis.</p> <p>Inspected the physical security policy to determine that policies and procedures were in place to guide personnel in physical security activities.</p> <p>Inspected the access request ticket for a sample of new hires and the written new hire process to determine that physical access was approved and granted to an employee as a component of the hiring process.</p> <p>Observed the entrance to the facility to determine that a manned reception desk was in place to monitor and control access to the entrance of the office facility during standard business hours.</p>	<p>Testing of the control activity disclosed that no employees were terminated during the review period.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>A badge access system controls access to and within the office facility.</p>	<p>Inspected the badge access listing and zone definitions to determine that a badge access system-controlled access to and within the facility.</p>	<p>No exceptions noted.</p>
		<p>Personnel are assigned to predefined badge access security zones based on job responsibilities.</p>	<p>Inquired of the President regarding physical access to determine that personnel were assigned to predefined badge access security zones based on job responsibilities.</p>	<p>No exceptions noted.</p>
		<p>The badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.</p>	<p>Inquired of the President regarding physical access monitoring to determine that the badge access system logged successful and failed access attempts, and that the logs could be pulled for review if necessary.</p>	<p>No exceptions noted.</p>
			<p>Observed the badge access system to determine that the badge access system logged successful and failed access attempts, and that the logs could be pulled for review if necessary.</p>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		Privileged access to the badge access system was restricted to authorized personnel.	Inquired of the President regarding privileged access to the badge access system to determine that privileged access to the badge access system was restricted to authorized personnel.	No exceptions noted.
		Access to the server room / data center is restricted to badge access cards assigned to authorized personnel.	Inspected the badge access administrator listing to determine that privileged access to the badge access system was restricted to authorized personnel.  Inquired of the President regarding critical system access to determine that access to the server room / data center was restricted to badge access cards assigned to authorized personnel.	No exceptions noted.
			Observed the badge access assignment restrictions to determine that access to the server room / data center was restricted to badge access cards assigned to authorized personnel.	No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		A video surveillance system is in place with footage retained for at least 90 days.	Inspected the server room / data center to determine that access to the server room / data center was restricted to badge access cards assigned to authorized personnel.  Inquired of the President regarding video retention to determine that a video surveillance system was in place with footage retained for at least 90 days.  Observed the oldest retained footage to determine that a video surveillance system was in place with footage retained for at least 90 days.  Inspected the video surveillance system configurations to determine that a video surveillance system was in place with footage retained for at least 90 days.	No exceptions noted.
		Visitors to the facility and server room are required to be escorted by an authorized employee.	Inquired of the President regarding visitor escorts to determine that visitors to the facility and server room were required to be escorted by an authorized employee.	No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Visitors are denied badge access to the system and must be monitored at all times by onsite staff.</p>	<p>Observed the visitor process throughout the facility to determine that visitors to the facility and server room were required to be escorted by an authorized employee.</p> <p>Inquired of the President regarding visitor access privileges to determine that visitors were denied badge access to the system and must be monitored at all times by onsite staff.</p> <p>Observed the visitor privilege and monitoring process to determine that visitors were denied badge access to the system and must be monitored at all times by onsite staff.</p>	<p>No exceptions noted.</p>
		<p>Visitors to the facility and server room are required to submit a helpdesk ticket prior to arrival.</p>	<p>Inquired of the President regarding visitor access requests to determine that visitors to the facility and server room were required to submit a helpdesk ticket prior to arrival.</p> <p>Observed the visitor access request process to determine that visitors to the facility and server room were required to submit a helpdesk ticket prior to arrival.</p>	<p>No exceptions noted.</p>
				<p>No exceptions noted.</p>



**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		Physical access to systems is revoked as a component of the termination process.	<p>Inspected the visitor tickets for a sample day and the physical security policy to determine that visitors to the facility and server room were required to submit a helpdesk ticket prior to arrival.</p> <p>Inquired of the President regarding access revocation to determine that physical access to systems was revoked as a component of the termination process.</p> <p>Inspected the sanction policies to determine that physical access to systems was revoked as a component of the termination process.</p> <p>Inspected the system and user access listing and termination request and checklist for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no employees were terminated during the review period.</p>
		User access to the badge access system is reviewed on an annual basis.	<p>Inspected the annual badge access review to determine that badge access reviews were completed by management on an annual basis.</p>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	<p>Policies and procedures are in place to guide personnel in data disposal and destruction.</p> <p>Badge access logs are maintained and monitored.</p> <p>Backup data is stored for a maximum of 90 days.</p>	<p>Inspected the data disposal and destruction policy to determine that policies and procedures were in place to guide personnel in data disposal and destruction.</p> <p>Inquired of the President regarding disposal requests to determine that backup data was stored for a maximum of 90 days.</p> <p>Inspected the backup retention policy to determine that backup data was stored for a maximum of 90 days.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	<p>Data that is no longer required for business purposes is deleted and overwritten.</p> <p>NAT functionality is utilized to manage internal IP addresses.</p>	<p>Inspected the data disposal and destruction policy to determine that data that was no longer required for business purposes was deleted and overwritten.</p> <p>Inspected the firewall configurations to determine that NAT functionality was utilized to manage internal IP addresses.</p>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>VPN, SSL and other encryption technologies are used for defined points of connectivity.</p> <p>VPN users are authenticated via individually-assigned user accounts and passwords.</p>	<p>Inspected the encryption configurations in place to determine that VPN, SSL and other encryption technologies were used for defined points of connectivity.</p> <p>Inquired of the President regarding VPN authentication to determine that VPN users were authenticated via individually-assigned user accounts and passwords.</p> <p>Observed an authorized user login to the remote access system to determine that VPN users were authenticated via individually-assigned user accounts and passwords.</p> <p>Inspected the VPN authentication configurations to determine that VPN users were authenticated via individually-assigned user accounts and passwords.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>
		<p>Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.</p>	<p>Inspected the encryption configurations for data in transit to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.</p>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inquired of the President regarding remote access to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		The firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configurations and an example automatic IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations in real-time.	Inspected the antivirus configurations to determine that the antivirus software was configured to scan workstations in real-time.	No exceptions noted.
		Critical data is stored in encrypted format.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format.	No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	<p>Logical access to stored data is restricted to authorized personnel.</p> <p>System backups are scheduled to run on a daily basis. Failed backups are automatically re-initiated up to three times.</p> <p>VPN, SSL and other encryption technologies are used for defined points of connectivity.</p> <p>Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.</p>	<p>Inquired of the President regarding data storage access to determine that access to stored data was restricted to authorized personnel.</p> <p>Inspected the user listing for the in-scope data storage infrastructure to determine that access to stored data was restricted to authorized personnel.</p> <p>Inspected the backup configurations to determine that system backups were scheduled to run on a daily basis, and failed backups were automatically re-initiated up to three times.</p> <p>Inspected the encryption configurations in place to determine that VPN, SSL and other encryption technologies were used for defined points of connectivity.</p> <p>Inspected the encryption configurations for data in transit to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the President regarding remote access to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Observed a user login to the remote access system to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
			Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	<p>The ability to implement changes into the production environment is restricted to authorized users.</p> <p>Backup media is stored in an encrypted format.</p>	<p>Inspected the firewall configurations to determine that NAT functionality was utilized to manage internal IP addresses.</p> <p>Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.</p> <p>Inspected the IDS configurations and an example automatic IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.</p> <p>Inspected the encryption configurations for data at rest to determine that backup media was stored in an encrypted format.</p> <p>Inquired of the President regarding production changes to determine that the ability to implement changes into the production environment was restricted to authorized users.</p> <p>Inspected the listing of privileged users to determine that the ability to implement changes into the production environment was restricted to authorized users.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Logical and Physical Access Controls**

<b>CC6.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Documented change control policies and procedures are in place to guide personnel in the change management process.</p> <p>Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.</p> <p>The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.</p> <p>The antivirus software is configured to scan workstations in real-time.</p>	<p>Inspected the change management policy to determine that documented change control policies and procedures were in place to guide personnel in the change management process.</p> <p>Inspected the antivirus software dashboard to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.</p> <p>Inspected the antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.</p> <p>Inspected the antivirus configurations to determine that the antivirus software was configured to scan workstations in real-time.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**System Operations**

<b>CC7.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC7.1	<p>To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.</p>	<p>Management has defined configuration standards in the information security policies and procedures.</p> <p>Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.</p> <p>The monitoring software is configured to alert IT personnel when thresholds have been exceeded.</p>	<p>Inspected the information security policy and the company intranet to determine that management had defined configuration standards in the information security policies and procedures.</p> <p>Inspected the monitoring system dashboard to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.</p> <p>Inquired of the President regarding system monitoring alerts to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.</p> <p>Inspected the centralized environmental monitoring system configurations and an example e-mail notification to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**System Operations**

<b>CC7.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configurations and an example automatic IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the incident response policy, the risk assessment policy, and the disaster recovery plan to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**System Operations**

<b>CC7.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	<p>Vulnerability scans are performed annually on the environment to identify control gaps and vulnerabilities.</p> <p>Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.</p> <p>Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.</p> <p>The monitoring software is configured to alert IT personnel when thresholds have been exceeded.</p>	<p>Inspected the completed vulnerability scan to determine that vulnerability scans were performed annually on the environment to identify control gaps and vulnerabilities.</p> <p>Inspected the incident response policy, the risk assessment policy, and the disaster recovery plan to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.</p> <p>Inspected the monitoring system dashboard to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.</p> <p>Inquired of the President regarding system monitoring alerts to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**System Operations**

<b>CC7.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>An IDS is utilized to analyze network events and report possible or actual network security breaches.</p>	<p>Inspected the centralized environmental monitoring system configurations and an example e-mail notification to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.</p>	<p>No exceptions noted.</p>
		<p>The IDS is configured to notify personnel upon intrusion detection.</p>	<p>Inspected the IDS configurations and an example automatic IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.</p>	<p>No exceptions noted.</p>
		<p>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.</p>	<p>Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.</p>	<p>No exceptions noted.</p>
		<p>Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.</p>	<p>Inspected the antivirus software dashboard to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.</p>	<p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**System Operations**

<b>CC7.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	<p>Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</p> <p>The antivirus software is configured to scan workstations in real-time.</p> <p>The incident response policies and procedures define the classification of incidents based on its severity.</p> <p>Resolution of incidents are documented within the ticket and communicated to affected users.</p>	<p>Inspected the antivirus configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.</p> <p>Inspected the antivirus configurations to determine that the antivirus software was configured to scan workstations in real-time.</p> <p>Inspected the incident response policy to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</p> <p>Inspected the incident response policy to determine that the incident response policies and procedures defined the classification of incidents based on its severity.</p> <p>Inspected the service desk tickets for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**System Operations**

<b>CC7.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.</p> <p>Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p>	<p>Inspected the service desk tickets for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.</p> <p>Inquired of the President regarding incident reviewal to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p> <p>Inspected the incident response policy to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**System Operations**

<b>CC7.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.  Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the incident response policy to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.  Inspected the service desk tickets for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.  No exceptions noted.  No exceptions noted.
		The actions taken to address identified security incidents are documented and communicated to affected parties.  Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the service desk tickets for a sample of incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.  Inspected the incident response policy and emergency contact list to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.



**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**System Operations**

<b>CC7.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Resolution of incidents are documented within the ticket and communicated to affected users.</p> <p>Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.</p> <p>Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p>	<p>Inspected the service desk tickets for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.</p> <p>Inspected the service desk tickets for a sample of incidents to determine that remediation actions taken for security incidents were documented within the ticket and communicated to affected users.</p> <p>Inquired of the President regarding incident reviewal to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**System Operations**

<b>CC7.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	<p>Change management requests are opened for incidents that require permanent fixes.</p> <p>Data backup and restore procedures are in place to guide personnel in performing backup activities.</p> <p>Control self-assessments that include backup restoration tests are performed on at least an annual basis.</p>	<p>Inspected the incident response policy to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p> <p>Inspected an example incident ticket requiring a permanent fix to determine that change management requests were opened for incidents that require permanent fixes.</p> <p>Inspected the backup policies to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.</p> <p>Inspected the completed backup restoration test to determine that control self-assessments that included backup restoration tests were performed on at least an annual basis.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**System Operations**

<b>CC7.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</p> <p>The disaster recovery plan is tested on an annual basis.</p> <p>The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.</p>	<p>Inspected the disaster recovery plan to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</p> <p>Inspected the disaster recovery test results to determine that the disaster recovery plan was tested on an annual basis.</p> <p>Inspected the disaster recovery plan and test results to determine that the business continuity and disaster recovery plan and procedures were updated based on disaster recovery plan test results.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Change Management**

<b>CC8.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	<p>Documented change control policies and procedures are in place to guide personnel in the change management process.</p> <p>The change management process has defined the following roles and assignments:</p> <ul style="list-style-type: none"> <li>• Authorization of change requests--owner or business unit manager</li> <li>• Testing-quality assurance</li> </ul> <p>The ability to implement changes into the production environment is restricted to authorized users.</p> <p>System changes are authorized and approved by management prior to implementation.</p>	<p>Inspected the change management policy to determine that documented change control policies and procedures were in place to guide personnel in the change management process.</p> <p>Inspected the change management policy to determine that the change management process defined the following roles and assignments:</p> <ul style="list-style-type: none"> <li>• Authorization of change requests--owner or business unit manager</li> <li>• Testing-quality assurance</li> </ul> <p>Inquired of the President regarding production changes to determine that the ability to implement changes into the production environment was restricted to authorized users.</p> <p>Inspected the listing of privileged users to determine that the ability to implement changes into the production environment was restricted to authorized users.</p> <p>Inquired of the President regarding change authorization to determine that system changes were authorized and approved by management prior to implementation.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Change Management**

<b>CC8.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>System change requests are documented and tracked in a ticketing system.</p> <p>System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.</p> <p>Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.</p>	<p>Inspected the change ticket for a sample of infrastructure changes to determine that system changes were authorized and approved by management prior to implementation.</p> <p>Inspected the change ticket for a sample of infrastructure changes to determine that system change requests were documented and tracked in a ticketing system.</p> <p>Inspected the change ticket for a sample of infrastructure changes to determine that system changes were tested prior to implementation and that the types of testing performed depended on the nature of the change.</p> <p>Inspected the change management policy and emergency contact list to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Mitigation**

<b>CC9.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	<p>Documented policies and procedures are in place to guide personnel in performing risk mitigation activities.</p> <p>Management has defined a formal risk management process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks, and defining specified risk tolerances.</p> <p>A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.</p>	<p>Inspected the risk assessment policy to determine that documented policies and procedures were in place to guide personnel in performing risk mitigation activities.</p> <p>Inspected the risk assessment policy to determine that management had defined a formal risk management process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks, and defining specified risk tolerances.</p> <p>Inquired of the President regarding the risk assessment to determine that a formal risk assessment was performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Mitigation**

<b>CC9.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Identified risks are rated using a risk evaluation process and ratings are approved by management.</p>	<p>Inspected the completed risk assessment to determine that a formal risk assessment was performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.</p> <p>Inquired of the President regarding risk identification to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.</p> <p>Inspected the risk assessment policy to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.</p> <p>Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.</p> <p>Inspected the risk assessment policy to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Mitigation**

<b>CC9.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	<p>Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.</p> <p>Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.</p>	<p>Inspected the vendor management policy to determine that management had defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.</p> <p>Inspected the vendor risk assessment reports for a sample of third-parties to determine that management developed third-party risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>Inspected the vendor risk assessment reports for a sample of third-parties to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Mitigation**

<b>CC9.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>The entity adheres to third-party agreements outline and communicate:</p> <ul style="list-style-type: none"> <li>• The scope of services</li> <li>• Roles and responsibilities</li> <li>• Terms of the business relationship</li> <li>• Communication protocols</li> <li>• Compliance requirements</li> <li>• Service levels</li> <li>• Just cause for terminating the relationship</li> </ul> <p>Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.</p> <p>A formal third-party risk assessment is performed for high-risk vendors to identify threats that could impair system commitments and requirements.</p>	<p>Inspected the vendor contracts for a sample of third-parties to determine that the entity adhered to third-party agreements outlined and communicated:</p> <ul style="list-style-type: none"> <li>• The scope of services</li> <li>• Roles and responsibilities</li> <li>• Terms of the business relationship</li> <li>• Communication protocols</li> <li>• Compliance requirements</li> <li>• Service levels</li> <li>• Just cause for terminating the relationship</li> </ul> <p>Inspected the third-party attestation report to determine that management obtained and reviewed attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.</p> <p>Inquired of the President regarding third-party risks to determine that a formal third-party risk assessment was performed for high-risk vendors to identify threats that could impair system commitments and requirements.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

**TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY**

**Risk Mitigation**

<b>CC9.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
			Inspected the vendor risk assessment reports for a sample of third-parties to determine that a formal third-party risk assessment was performed for high-risk vendors to identify threats that could impair system commitments and requirements.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY				
A1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.  The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring system dashboard to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.  Inquired of the President regarding system monitoring alerts to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.  Inspected the centralized environmental monitoring system configurations and an example e-mail notification to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.	No exceptions noted.  No exceptions noted.  No exceptions noted.
		Processing capacity is monitored 24x7x365.	Inspected the monitoring tool configurations to determine that processing capacity was monitored 24x7x365.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY				
A1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	<p>The change management process is followed when a change is made to a system as a result of capacity constraint.</p> <p>Environmental threats (e.g. floods, fires, electrical discharge, etc.) that could impair the availability of the system are considered and identified as a part of the risk assessment process.</p>	<p>Inspected the load-balancing statement through the entity's website and a change ticket for an example change made to a system as a result of a capacity constraint/issue to determine that the change management process was followed when a change was made to a system as a result of capacity constraint.</p> <p>Inspected the risk assessment policy to determine that environmental threats that could impair the availability of the system were considered and identified as a part of the risk assessment process.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>

ADDITIONAL CRITERIA FOR AVAILABILITY				
A1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>A centralized environmental monitoring system is in place to monitor facilities housing production systems and send automated alerts to personnel if pre-defined thresholds are exceeded.</p> <p>Temperature and humidity sensor systems are in place in the facility that notifies operations support personnel via e-mail of readings outside of the defined parameters.</p>	<p>Inquired of the President regarding environmental system monitoring alerts to determine that a centralized environmental monitoring system was in place to monitor facilities housing production systems and send automated alerts to personnel if pre-defined thresholds are exceeded.</p> <p>Inspected the centralized environmental monitoring system configurations and an example e-mail notification to determine that a centralized environmental monitoring system was in place to monitor facilities housing production systems and send automated alerts to personnel if pre-defined thresholds are exceeded.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p>
			<p>Inspected the centralized environmental monitoring system configurations and an example e-mail notification to determine that temperature and humidity sensor systems were in place in the facility that notified operations support personnel via e-mail of readings outside of the defined parameters.</p>	<p>No exceptions noted.</p>

<b>ADDITIONAL CRITERIA FOR AVAILABILITY</b>				
<b>A1.0</b>	<b>Criteria</b>	<b>Control Activity Specified by the Service Organization</b>	<b>Test Applied by the Service Auditor</b>	<b>Test Results</b>
		<p>Fire detection and prevention systems are present throughout the facility including smoke detection devices, hand held fire extinguishers, and pre-action dry pipe fire suppression.</p>	<p>Observed the fire detection and prevention systems within the office facility/data center facilities to determine that fire detection and prevention systems were present throughout the office facility/data center including smoke detection devices, hand held fire extinguishers, and pre-action dry pipe fire suppression.</p>	<p>No exceptions noted.</p>
		<p>The pre-action dry pipe fire suppression systems are tested and inspected by a third-party on an annual basis.</p>	<p>Inquired of the President regarding annual fire inspections to determine that the pre-action dry pipe fire suppression systems were tested and inspected by a third-party on an annual basis.</p>	<p>No exceptions noted.</p>
		<p>Handheld fire extinguishers are inspected on an annual basis to ensure that the pressure is within the recommended levels.</p>	<p>Inquired of the President regarding annual fire extinguisher inspections to determine that handheld fire extinguishers were inspected on an annual basis to ensure that the pressure was within the recommended levels.</p>	<p>No exceptions noted.</p>

ADDITIONAL CRITERIA FOR AVAILABILITY				
A1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The data center facilities are equipped with raised flooring to elevate equipment and help facilitate cooling.	Inspected the completed fire inspection reports to determine that handheld fire extinguishers were inspected on an annual basis to ensure that the pressure was within the recommended levels.	No exceptions noted.
		The data center facilities are equipped with a leak detection system to detect water in the event of a flood or water leakage.	Observed the raised flooring within the data center facilities to determine that the data center facilities were equipped with raised flooring to elevate equipment and help facilitate cooling.	No exceptions noted.
		An uninterruptible power supply (UPS) is in place to provide power to critical infrastructure equipment in the event of a temporary power loss or power surge.	Inquired of the President regarding power support devices to determine that a UPS was in place to provide power to critical infrastructure equipment in the event of a temporary power loss or power surge.	No exceptions noted.
			Observed the leak detection system within the data center facilities to determine that the data center facilities were equipped with leak detection systems to detect water in the event of a flood or water leakage.	No exceptions noted.
			Inquired of the President regarding power support devices to determine that a UPS was in place to provide power to critical infrastructure equipment in the event of a temporary power loss or power surge.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY				
A1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>The UPS units are inspected and maintained by a third-party on an annual basis.</p> <p>Generators fueled by diesel fuel are in place to provide power to the data center in the event of an extended power outage.</p> <p>The generators are tested on a weekly basis.</p> <p>Preventive maintenance inspections and service is performed on the generators by a third-party on a quarterly basis.</p>	<p>Observed the UPS units to determine that a UPS was in place to provide power to critical infrastructure equipment in the event of a temporary power loss or power surge.</p> <p>Inspected the completed maintenance report to determine that the UPS units were tested and inspected by a third-party on an annual basis.</p> <p>Observed the generator to determine that generators fueled by diesel fuel were in place to provide power to the data center in the event of an extended power outage.</p> <p>Inquired of the President regarding generator tests to determine that the generators were tested on a weekly basis.</p> <p>Inspected generator testing results for a sample of weeks to determine that the generators were tested on a weekly basis.</p> <p>Inspected maintenance reports for a sample of quarters to determine that the generators were inspected by a third-party on a quarterly basis.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>



ADDITIONAL CRITERIA FOR AVAILABILITY				
A1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>The facility is equipped with multiple Heating Ventilation and Air Conditioning (HVAC) units that provide redundancy in the event of one unit's failure.</p>	<p>Inquired of the President regarding HVAC redundancy to determine that the data center facilities were equipped with multiple HVAC units that provided redundancy in the event of one unit's failure.</p>	<p>No exceptions noted.</p>
		<p>The HVAC units are inspected and maintained by a third-party on an annual basis.</p>	<p>Observed the onsite HVAC units to determine that the data center facilities were equipped with multiple HVAC units that provided redundancy in the event of one unit's failure.</p>	<p>No exceptions noted.</p>
		<p>Alerts generated from the centralized environmental monitoring system are sent to operations support personnel that are responsible for investigating and resolving the alerts.</p>	<p>Inspected the annual HVAC maintenance report to determine that the HVAC units were inspected by a third-party on an annual basis.</p>	<p>No exceptions noted.</p>
		<p>Environmental protection policies and procedures are documented and maintained.</p>	<p>Inspected the centralized environmental monitoring system configurations and an example e-mail notification to determine that alerts generated from the centralized environmental monitoring system were sent to operations support personnel that were responsible for investigating and resolving the alerts.</p>	<p>No exceptions noted.</p>
		<p>Environmental protection policies and procedures are documented and maintained.</p>	<p>Inquired of the President regarding environmental policy reviewal to determine that environmental protection policies and procedures were documented and maintained.</p>	<p>No exceptions noted.</p>

ADDITIONAL CRITERIA FOR AVAILABILITY				
A1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>System backups of critical components are scheduled to run on a daily basis. Failed backups are automatically re-initiated up to three times.</p> <p>When a backup job fails, the backup tool sends an alert via service desk ticket to network operations center, who investigate and resolve the failure.</p> <p>Redundant architecture is in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.</p>	<p>Inspected the environmental protection policies and procedures to determine that environmental protection policies and procedures were documented and maintained.</p> <p>Inspected the backup configurations to determine that system backups of critical components were scheduled to run on a daily basis, and failed backups were automatically re-initiated up to three times.</p> <p>Inspected backup configurations and an example backup alert to determine that when a backup job failed, the backup tool sent an alert via service desk ticket to network operations center, who investigated and resolved the failure.</p> <p>Inspected the business continuity and disaster recovery plans and network diagram to determine that redundant architecture was in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>

ADDITIONAL CRITERIA FOR AVAILABILITY				
A1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	<p>The disaster recovery plan includes moving the business operations and supporting systems to a hot site.</p> <p>A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.</p> <p>The disaster recovery plan is tested on an annual basis.</p> <p>Data backup restoration tests are performed at least annually.</p>	<p>Inspected the business continuity and disaster recovery plans to determine that the disaster recovery plan included moving the business operations and supporting systems to a hot site.</p> <p>Inspected the disaster recovery plan to determine that a business continuity plan was documented and in place that outlined the range of disaster scenarios and steps the business would take in a disaster to ensure the timely resumption of critical business operations.</p> <p>Inspected the disaster recovery test results to determine that the disaster recovery plan was tested on an annual basis.</p> <p>Inspected the completely completed backup restoration test results to determine that data backup restorations were performed at least annually.</p>	<p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p>