



A Proposal to Provide  
**Call Center Support Services  
for ACCESSNebraska**

RFP# 113578 O3 ■ December 6, 2022

Prepared for

**NEBRASKA**

Department of Health and Human Services

by Gatestone & Co. International, Inc.

December 6, 2022

State of Nebraska  
Department of Health and Human Services  
301 Centennial Mall S, Suite 500  
Lincoln, NE 68509  
Attn: Rene A. Botts / Carrie DeFreece

**RE: RFP 113578 O3 for ACCESSNebraska Call Center Support**

**EXECUTIVE SUMMARY**

On behalf of Gatestone & Co. International, Inc. (“Gatestone”), we are pleased to provide our proposal to the State of Nebraska in response to RFP 113678 O3 for ACCESS Nebraska Call Center Support. We confirm that this response outlines Gatestone’s extensive call center experience, particularly within the government sector in North America. With our local Omaha presence, we are a provider with the capability of providing flexible, accessible service and availability.

Gatestone is North America’s first and most experienced BPO and call center supplier. The company has been providing call center, business process outsourcing, and receivable management services globally since 1926. Our response will provide the relevant information on Gatestone’s demonstrated ability to provide call center services, supported by qualified and well-trained resources and a highly secure infrastructure and architecture. As one of the largest call center providers in North America, Gatestone has gained tremendous experience working with government, financial services, telecommunications and major brand companies in provision of call center services. We are well-poised to offer delivery of exceptional call center services to support Nebraska’s contract call center needs. Our services are offered with the robust data security and technology safeguards required to protect clients, while delivering customer satisfaction with every interaction.

Throughout this document, we intend to reinforce our commitment to supporting the delivery of this critical service on the State’s behalf. We bring the maturity, financial strength, technological sophistication, and human resources expertise to proudly deliver programs that work. In coordination with our hub in Omaha, Nebraska, ACCESSNebraska will also be supported by “Gatestone@Home,” our remote working solution incorporating the required tools and resources, sophisticated workplace security standards, and a cloud-based virtual environment for demand management, flexibility and efficiency. We acknowledge and fully agree with the State’s position which helps address the real and perceived risks to confidentiality, privacy, and cybersecurity, particularly for an initiative such as this. We also commit to delivering Gatestone@Home services by hiring Nebraska-based resources on a first and full priority basis, as required.

The table below highlights some of the features and benefits that come from entrusting Gatestone with ACCESSNebraska’s Call Center Support program:



FEATURES	BENEFITS
✓ <b>Qualified call center service experience with proven track record of success</b>	= ACCESSNebraska will benefit from Gatestone's exceptional knowledge, effective call center processes, best practices, and compliance. We have gained tremendous experience and knowledge supporting almost one hundred government entity programs, each with their own unique and distinct work requirements.
✓ <b>Most experienced management team</b>	= Our highly experienced management team, with more than 25 years of average tenure, has expertise in onboarding and executing a wide variety of multifaceted call center programs. Our management team has honed and refined processes and developed strong working relationships across the company, with exceptional program performance.
✓ <b>Better than industry standard compensation</b>	= Our agents receive compensation at higher levels than industry standard, meaning that we have higher retention than the rest of the industry. This results in less need to train new agents as well as better customer service, higher customer satisfaction, better overall call times and the greater likelihood that any issue will be addressed in a single call.
✓ <b>Solid recruitment, qualification and hiring process</b>	= We will utilize highly qualified agents identified as the most likely to succeed in your program. Our resources will be selected and approved using the Gatestone Index ("GI") with agent profiles matched against job descriptions and similar client programs. Selected agents will be well-trained to act professionally, effectively, and compliantly on all matters of your business. Our aim is to provide the best workplace experience and environment for our employees, in turn lowering turnover and increasing our already high average agent tenure.
✓ <b>We are extremely innovative</b>	= With continuous investment in state-of-the-art networking systems, world-class data security, proprietary software, E-Learning training systems, Artificial Intelligence (AI) and exciting new technology and communication applications, we will create ease of use in communicating with ACCESSNebraska's customers.
✓ <b>We are committed to security and to standards</b>	= Gatestone holds PCI Level 1, ISO 27002, SOC 1, SOC 2 and HIPAA certifications. We operate within a secure environment and treat privacy and confidentiality as a top priority. Gatestone is pursuing further security standards including ISO 27018. We bring the full weight of our capabilities and controls and draw upon the expertise of our team to monitor, manage, and mitigate risks.

✓ **We are focused on elevated levels of quality control and compliance testing**

= The State of Nebraska benefits from our robust Compliance and Quality Assurance departments and corresponding controls which ensure program workflows, procedures and actions are consistent with the agreed upon expectations. This reduces any potential risk to the State.

*We acknowledge receipt of Addendum 1, dated November 2, 2022, and Addendum 2, dated November 16, 2022.*

In closing, we thank you for this opportunity. Gatestone looks forward to establishing business relationship with ACCESSNebraska on this initiative. You have our commitment to deliver an elevated partner experience providing success across all levels of our operations.



---

Spencer Wilson  
*Senior Vice President*  
Direct: 1-800-900-4238 x 2993  
Email: [spencer.wilson@gatestonebpo.com](mailto:spencer.wilson@gatestonebpo.com)



# 1. Corporate Overview

1. CORPORATE OVERVIEW

a. CONTRACTOR IDENTIFICATION AND INFORMATION

RFP Language: 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.

Corporate Name: Gatestone and Co. International, Inc.
Domestic Headquarters: 260-455 N 3rd Street, Suite 260, Phoenix, AZ 85004
Entity Organization: Corporation
State of Organization: Delaware
Year of Organization: 1926
Name/Form Changes: N/A

b. FINANCIAL STATEMENTS

RFP Language: 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.

Our 2021 combined financial statements are included in a separate document as they are considered to be confidential and proprietary information. Gatestone has no judgments pending nor any expected litigation, or other real or potential financial reversals which might materially affect the viability or stability of the organization.

c. CHANGE OF OWNERSHIP

RFP Language: 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.



No such acquisitions are anticipated to occur within the next twelve months or at any time subsequent to that.

## d. OFFICE LOCATION

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

Gatestone's call center location in Omaha, Nebraska, located at 7015 L Street, Omaha, NE 22407 is fully-equipped to fulfill the requirements of this RFP.

## e. RELATIONSHIPS WITH THE STATE

*RFP Language:* 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.

Gatestone does not have any existing contracts with the State of Nebraska.

## f. BIDDER'S EMPLOYEE RELATIONS TO STATE

*RFP Language:* 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.

No such relationships exist.

## g. CONTRACT PERFORMANCE

*RFP Language:* 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.

Gatestone has not had any contracts terminated during the past 5 years.

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

*RFP Language:* 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.

**Note:** As their standard operating procedure, our Public Sector clients and a number of our Private Sector clients do not, and will not, provide references under any circumstances. ***This being the case, our references are contained in a separate document and are to be considered confidential and proprietary.*** Given the vast nature of our public sector call center experience, Gatestone would welcome an in-depth discussion with the State and our operations executives to fully detail our experience and capabilities in this regard. We would not want the State to miss the opportunity for a qualified and experienced vendor when coming to something as sensitive as ACCESSNebraska.

---

***Gatestone has performed on all of these programs as the prime consultant.***

---

*RFP Language:* ii. Bidder and Subcontractor(s) experience should be listed separately. Narrative descriptions submitted for Subcontractors should be specifically identified as Subcontractor projects.

Not applicable – our experience is being submitted as the prime contractor with no subcontractors.





**RFP Language: 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.

Not applicable – our experience is being submitted as the prime contractor with no subcontractors.

## **i. SUMMARY OF BIDDER'S PROPOSED PERSONNEL / MANAGEMENT APPROACH**

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

Gatestone's recruitment and hiring process uses an organizational socialization methodology by which people learn about and adjust to the knowledge, skills, attitudes, expectations, and behaviors needed for a new or changing role within Gatestone. We use proven HR Services to source, assess, hire, track, and onboard new employees with the requisite knowledge, skills, and qualities to perform work and handle complex situations. This includes assessment of academic background as well as previous experience. As part of the hiring process, or prior to transferring an employee to a new role, Gatestone will undertake a proprietary **Gatestone Index (GI)** behavioral assessment survey, which profiles individual characteristics and strengths matched to a job profile. This will include language, soft skills competencies, and other abilities such as effective communication, attention to detail, problem solving, sales ability, and more. This survey is administered to every potential candidate and employee at Gatestone and provides analytical information on their potential to succeed within a specific role.

Gatestone's strategy to hire, train and retain call center staff is demonstrated through its almost 100 years' Human Resources (HR) experience in implementing successful call center projects. Gatestone has documented its achievements, best practices as well as lessons learned, from each onboarding experience it has undertaken since 1926.

The company's recruitment and hiring process is a function of the HR department and is managed by the Director of HR with assistance from a large global team of recruiting and resourcing managers, HR supervisors, employee engagement specialists, training and development managers, and administrative support staff.

All training and education programs are managed by our training manager, supported by a team of dozens of training professionals who work together to develop and administer Gatestone's training and development programs, as well as, training related to internal and client policies and procedures and each client program's Statement of Work (SOW) including the Key Performance Indicators (KPI) and Service Level Agreement (SLA). Our typical training program consists of 2-weeks initial virtual or classroom training, followed by 30 days' on-the-job (OJT) training and knowledge transfer training across roles, further followed-up with ongoing training after 60-90 days.

Gatestone retention strategy includes implementing several initiatives and incentives with the goal of reinforcing our organizations culture, supporting company goals and values and recognizing the many employees who go above and beyond. Gatestone employs a team of full-time dedicated employee engagement specialists responsible for internal communication projects, employee incentives, corporate savings programs and motivational campaigns. Examples of the employee retention programs we have in

place are performance incentives, employee recognition and gift rewards, preferential scheduling, opportunity to engage in formal employee management training programs, access to employee scholarship programs, and employee milestone gift rewards, to name a few. Since implementing these strategies, we have seen a significant increase in retention, year over year with agent average tenure trending around 6 years, which is way above industry standard.

### Project Manager Roles and Responsibilities

The Project Manager's roles and responsibilities will include:

- Holding the authority to commit necessary resources, build technology infrastructure, hire and manage the workforce, and implement associated processes for the program
- Working with core departments such as call center operations, client solutions, quality control and compliance, human resources, program management, risk management, workforce management, information technology, training, and finance
- Ensuring clear and complete understanding of all program requirements
- Determining the tasks necessary for meeting those requirements
- Managing and executing the Project Implementation Plan including program development and implementation through to launch
- Maintaining updating, and distributing the Project Implementation Plan to program team members
- Developing a proactive Communication Plan for the engagement which includes status reporting and other communication methods such as meetings and informal communications within the Project Implementation team and the State
- Providing project performance reporting documenting the project's performance against the plan, which includes reporting on activities such as quality and risk management
- Coordinating with the State and direct task completion
- Assessing potential risks and select alternative courses of action to attain the stated goals of the program
- Managing and monitoring issue and change management
- Ensuring that the project is completed on time (or ahead of schedule) and exceeds the State's expectations
- Holding quarterly and other formal business reviews to analyze a summary of the relationship, to develop plans and strategies for the future, to review and evaluate ongoing specific projects, and to discuss any upcoming strategic business initiatives.

The Project Manager also has the authority to commit necessary resources, build technology infrastructure, hire and manage the workforce, and implement associated processes for the project. Rigorous attention to detail and regularly scheduled program reviews with the State will be employed throughout implementation to keep the project on schedule. Our project team departments will also be available to assist with the implementation and identifying continuous improvement opportunities from implementation to ongoing operations.



## Project Team

**RFP Language:** 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.

Below we have provided bios of our qualified and long-tenured management team who are in place and currently managing Gatestone's call center contracts. These individuals are the key personnel we are proposing for the ACCESSNebraska project. All individuals have several years to decades worth of experience supporting similar size and scope services.

### ***John Tilley, President***

John Tilley began his career at Gatestone in 1980. Over the years he has been promoted to more senior management roles, now serving as President of Gatestone's global customer contact facilities. As President of Gatestone, John is responsible for client performance, overall company internal controls and risk mitigation. John ensures our customer-facing agents operate within our ethical business conduct guidelines, as well as within all legal and regulatory compliance. John also ensures our agents understand KPI and service level expectations as they deliver excellent customer experience. John is a frequent guest speaker at industry forums throughout North America, and is widely respected for his analytical approach to our customer service performance.

### ***Peter Kines, Executive Vice President & CFO***

Peter Kines is an accomplished finance professional with broad industry experience in corporate financing, operational financial management, strategic planning, and business development. He is a CPA who brings an informed approach gained working in technology, telecommunications, and outsourced labor services industries, to name a few. Peter is a resourceful problem solver who, with his collaborative leadership style, has the ability to lead and implement effective solutions for business issues. With knowledge gleaned from previous experience as the CFO of several large companies, Peter works closely with Gatestone's operations department to plan and budget resources efficiently. His core purpose is to ensure that appropriate resources will be available for each contract and that they are deployed in the most efficient manner to ensure success.

### ***Alexander Wilson, LL. B, LL.M, Vice President, Legal & Compliance***

Alexander currently oversees the company's Legal & Compliance Department and Ombudsman Office. Through his extensive expertise, he skillfully undertakes all of Gatestone's compliance, corporate licensing, contract review, and litigation. Alexander exercises management responsibility for ongoing compliance monitoring with the scope of the company's code of professional conduct, policies, and procedures. He acts as an interface with the audit department as they perform periodic compliance audits. Alexander also provides guidance to managers and staff regarding control procedures and testing and assists the President with identifying compliance risks and in implementing plans to monitor and address risks.

***Anna Donnelly, Vice President, US Operations***

With a rich background in business, data, finance, and process management through positions relating to accounting, data production, and internal auditing, Anna has worked in a number of capacities within the customer service industry. She has more than 25 years of expertise with Gatestone and has been promoted to more senior, supervisory, and management roles within the Operations division, now serving as Vice President. Anna's strength lies in her organizational skills and her ability to manage various sites and projects. Her successes include her ability to develop and manage support staff and processes to drive strong performance resulting in substantial program growth and repeat client contract renewals.

***Durea Falkner, Director, Omaha Operations***

As the Director of Operations for almost 10 years at our Omaha, Nebraska site, Durea oversees day to day call center operations. He is responsible for the daily production of the frontline team of full-time agents, providing stellar results with 100% compliance. This includes providing support in the hiring and training of all new staff, as well as implementing innovative and unique methods to maximize production while maintaining a payroll budget. Durea's strong attention to detail and prior management experience provides the capability of achieving all client KPI and SLA results while staying in compliance with State and Federal regulations. His commitment to execution and time management ensures that his staff is ready and able to perform all requirements of their positions which includes monthly refresher training and one-on-one coaching and development.

***Ali Khan, Vice President, Information Technology Infrastructure***

Ali Khan is an accomplished IT leader with more than a decade of experience, a deep knowledge of technology, and extensive experience across multiple functions such as network administration, system integration, development and setup, among others. His skill set lends itself to his exceptional problem-solving and troubleshooting abilities, which have helped Gatestone establish a technologically advanced call center. As Vice President of IT Infrastructure, Ali has been critical to the roadmap for the Information Technology future of Gatestone. He is responsible for network and server administration, help desk, telecom, and security. Ali was the key architect for Gatestone's many successful infrastructure solutions for all of our long-standing clients. As he continues to bring new changes to our environment, he has designed our current structure and has begun putting in place the vision for the Gatestone infrastructure for the future.

***Dayira Quiel, Director, Client & Support Services***

Dayira Quiel is the Director of Client & Support Services with more than a decade of customer support experience. Dayira manages Gatestone's Client & Support Services team which is deeply committed to ensuring a successful outcome for every client. Her purpose is to serve as a key strategic liaison and project manager, overseeing client inquiries through resolution at the client's satisfaction including provision of all reporting requirements for the program. Dayira holds a wealth of experience across a number of back-office and support services facets, along with substantial knowledge of industry regulations. She uses this skill and knowledge to manage procedure development, implementation, and client services for all clients.



### ***Suzanne Huether, Director, Human Resources***

Suzanne has been with Gatestone for 20 years and is responsible for overseeing the Human Resources Department function and supervising the employees. Suzanne manages the administration of employee contracts, on-boarding, employee files, compensation and benefits, recruitment, selection, training, and development. She also ensures company compliance with regulatory and client-based employment standards. Suzanne holds a BA in Sociology from McMaster University and a Diploma in Business Administration with focus on HR Management from Algonquin College. She was granted her Certified Human Resources Professional (CHRP) designation in September 2012 by the Human Resources Professional Association.

### ***Chelsea Soulier, Manager, Human Resources***

Chelsea holds more than seven years of experience managing Human Resources departments and provides employee relations guidance and leadership and is responsible for talent acquisition, the administration of employee contracts, on-boarding, employee files, benefits. She also ensures compliance with regulatory and client-based employment standards. Chelsea is a member of the Society for Human Resource Management.

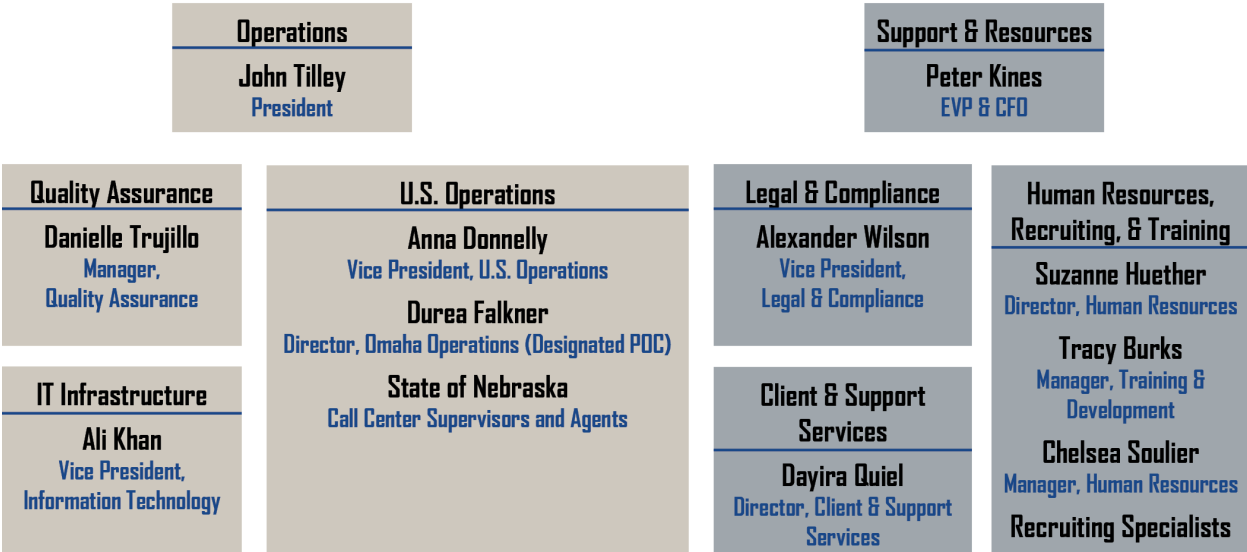
### ***Danielle Trujillo, Manager, Quality Assurance***

As a Quality Manager with Gatestone for more than 15 years, Danielle implements programs that enable Gatestone to deliver quality standards that exceed client expectations. She works closely with the Operations Manager assigned to projects to guide supervisors and employees on policy interpretation, performance management, disciplinary processes, and adherence to State and Federal regulations. Danielle has developed training that focuses on improving customer satisfaction standards based on State and Federal procedures and established guidelines that impact call calibration sessions, monitoring standards and compliance training.

### ***Tracy Burks, Manager, Training & Development***

Tracy Burks oversees our training department and develops Gatestone's customer service training programs to ensure comprehensive instruction on all protocols, Gatestone policies and procedures, and client-specific requirements. Tracy has been directly involved in developing and providing training to our employees since 2006. She is actively involved in a number of industry organizations in order to remain current and knowledgeable on regulations and best practices in call center operations and training techniques. Tracy holds her Six Sigma Lean Professional, Corporate Trainer Certified, and Change Management Specialist certifications.

Organization Chart



**RFP Language:** 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.

Resumes for all of the proposed individuals are included in the content that follows. The confidential references provided previously are personnel references, as well as corporate references.

**j. SUBCONTRACTORS**

**RFP Language:** 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.

Gatestone will not require the use of subcontractors to perform the work of this contract.





## John Tilley

### President – Operations Leader



John Tilley began his career at Gatestone in 1980 and holds 12 years' experience serving as President and primary Client contact at Gatestone. Starting his extensive career at the firm as a collection agent, he has been promoted to senior management roles, currently serving as President of Gatestone's global operations. As President, John is responsible for overseeing the company's network of offices throughout North America, Central America and Asia, overall client performance and corporate strategy. John is responsible for the successful onboarding and continued oversight of hundreds of projects. John's office is located on the collection production floor and he maintains an open-door policy for all. John has managed and successfully delivered numerous diverse national debt collection client portfolios including government, financial services, retail, and utility programs, which includes all the varying collection account levels. John is responsible for overseeing the debt collection contracts for each of the five big banks in Canada, a National Master Standing Offer with the Government of Canada, and approximately 40 individual government departments, and all the major telecommunications companies in Canada.

#### Areas of Expertise

- Corporate oversight
- Client performance
- Corporate strategy
- Client onboarding
- Debt collection services operation

#### Professional Registrations / Affiliations

Canadian Society of Collection Agencies  
American Collectors Association  
Credit Counseling Canada

#### Role & Responsibilities

John ensures our customer-facing agents operate within our ethical business conduct guidelines, and he ensures legal and regulatory compliance. John is a frequent guest speaker at industry forums throughout North America, and he is widely respected for his analytical approach to collections performance. John is responsible for maintaining overall client oversight and ensuring that all contract deliverables are met. He ensures that the agents operate within ethical guidelines, understand KPIs, and deliver excellent customer service.



## Peter Kines, CPA

### Vice President & CFO

#### Areas of Expertise

- Financial management
- Business solutions
- Resources budgeting
- Resource management

#### Certifications/Licenses

Chartered Professional Accountant (CPA)

Peter Kines is an accomplished finance professional with broad industry experience in corporate financing, operational financial management, strategic planning, and business development. He is a CPA who brings an informed approach gained working in technology, telecommunications, and outsourced labour services industries, to name a few. Peter is a resourceful problem solver who, with his collaborative leadership style, has the ability to lead and implement effective solutions for business issues. With knowledge gleaned as the CFO of several large companies, Peter works closely with Gatestone's Operations department to plan and budget resources efficiently. His core purpose is to ensure that appropriate resources will be available for each contract and that they are deployed in the most efficient manner to ensure success.

#### Role & Responsibilities

Peter's extensive experience lends itself towards the strategic management of the accounting and finance functions at Gatestone. He directs accounting policies, procedures and internal controls while recommending improvements to ensure the integrity of a company's financial information. Peter manages or oversees the relationship with independent auditors and collaborates with Gatestone's executive team on business decisions. He oversees financial systems implementations and upgrades and identifies and manages business risks and insurance requirements. As well, Peter oversees the preparation of all financial reporting and advises on long-term business and financial planning.





## Danielle Trujillo

*Manager, Quality Assurance*



As Chief Compliance Officer, Danielle oversees and manages all aspects of compliance across the company ensuring Gatestone is operating within all regulatory requirements as well as the company's internal Policies and Procedures. She is responsible for overseeing Gatestone's Compliance department and has developed Gatestone's compliance strategy, structure, and processes.

### *Role and Responsibilities*

#### Areas of Expertise

- Regulatory compliance
- Policy development
- Training program development
- Compliance review

#### Time with Firm

Since 2004

- Propagates compliance strategies and responsibilities
- Establishes standards and implements procedures to ensure the compliance programs throughout the company are effective in identifying, preventing, detecting, and correcting non-compliance with all applicable rules and regulations and contract directives as well as the company's internal policies and procedures
- Maintains current knowledge of laws and regulations, keeping abreast of recent changes
- Develops policies and programs that encourage managers and employees to report suspected fraud and other improprieties without fear of retaliation
- Periodically revises the compliance program when operational changes, regulatory changes, or company policy and procedure changes occur
- Develops, coordinates, and participates in continuous educational and training programs that focus on the elements of the company's compliance program
- Ensures all employees within the compliance department are trained and knowledgeable about all compliance policies and procedures and comply with them
- Develops materials at an institutional level for distribution to all employees to enhance awareness of compliance activities
- Coordinates internal compliance review and monitoring activities, including periodic reviews of the department
- Responds to government investigations and queries as the principal point of contact
- Independently investigates and acts on matters related to compliance, including the flexibility to design and coordinate internal investigations
- Monitors external audit review processes, maintains awareness of compliance issues, and responds to administrative inquiries related to compliance issues or audits.



## Ali Khan

### Vice President, Information Technology



Ali Khan is an accomplished IT leader with more than a decade of experience, a deep knowledge of technology, and extensive experience across multiple functions such as network administration, system integration, development and setup, among others. His skill set lends itself to his exceptional problem-solving and troubleshooting abilities, which have helped Gatestone establish a technologically advanced contact centre. As Vice President of IT Infrastructure, Ali has been critical to the roadmap for the Information Technology future of Gatestone. He is responsible for network and server administration, help desk, telecom, and security. Ali was the key architect for Gatestone's many successful infrastructure solutions for all of our long-standing clients. As he continues to bring new changes to our environment, he has designed our current structure and has begun putting in place the vision for the Gatestone infrastructure for the future.

#### Areas of Expertise

- Network setup and maintenance
- Technical support
- Network monitoring
- Routing protocols
- Technology configuration and maintenance
- ERP software
- Technical writing

#### Education

**Bachelor of Math** – Mathematics,  
University of Waterloo, 2016

#### Time with Firm

Since 2015

#### Certifications/Licenses

Cisco Certified Network Associate  
(CCNA)

#### Role and Responsibilities

As the head of Gatestone's Information Technology department, composed of approximately 25 FTE, Ali is responsible for the overall support of network, telephony, help desk and CRM application systems across multiple offices in Canada, USA, Latin America and Asia. With his extensive knowledge, Ali reengineered the company network infrastructure, to produce a stable and secure environment, thereby reducing incidents. As well, he has been instrumental towards introducing budget and cost tracking software.



## Anna Donnelly

### Vice President – U.S. Operations



With a rich background in business, data, finance, and process management through positions relating to accounting, data production, and internal auditing, Anna has worked in a number of capacities within the accounts receivable/contact center management industry. Anna has more than 25 years' expertise with Gatestone and has been promoted to more senior, supervisory and management roles within the Operations division, now serving as Vice President. Anna has an Associate of Accounting Technicians designation, as well as a degree in Business Management and Finance.

Anna's strength lies in her organizational skills and her ability to manage various sites and projects. Her successes include her ability to develop and manage support staff and processes to drive strong performance resulting in substantial program growth and repeat client contract renewals.

#### Areas of Expertise

- Accounting
- Data production
- Internal auditing
- Staff development

#### Education

**B.A.** – Business Management and Finance, Wirral College, 1998

**Associate** – Accounting Technician,

#### Time with Firm

Since 2002

#### Role & Responsibility

Anna collaborates with the executive team to develop debt collection/contact center support structures for each program within her area of responsibility while directing the operations team on Gatestone's mission, values, and strategic goals. She participates in the hiring and training of support team members and provides continuous leadership, training, and professional support to a team of managers and support staff across all sites and programs. Anna also actively participates in onboarding of new programs including contributing to new process development.

Anna's responsibilities include developing business and financial strategies for her areas of responsibility and is vital towards the achievement of targets, budgets, and performance goals. Her oversight into strategies and tactical activities of Gatestone's locations and teams is crucial towards maximizing operating performance and maintaining customer relationships. Additionally, Anna works with teams to ensure staffing redundancy in all major functions and ensures process documentation for all key roles and responsibilities within her areas of responsibility.

Anna participates in client business review meetings and engages in escalation paths for clients. She evaluates performance and provides feedback for improvement and development to members of the leadership team. Anna maintains an awareness of relevant industry and market changes and proactively implements mitigation measures to maintain or improve performance levels.



## Durea Falkner

### Director, Omaha Operations



As a Director of Operations, Durea oversees day-to-day operations to provide stellar results for our clients. He is responsible for the daily production of the frontline team of full-time agents, providing stellar results with 100% compliance. This includes support in the hiring and training of all new staff members, as well as implementing innovative and unique methods to maximize production while maintaining a payroll budget. Durea's strong attention to detail and prior management experience provide the capability for achieving results while staying in compliance with State and Federal regulations. His commitment to execution and time management ensures that his staff is ready and able to perform all requirements of their position which includes monthly refresher training and one-on-one coaching and development.

#### Areas of Expertise

- Supervision
- Workflow building
- Recruiting
- Budgeting
- Compliance

#### Education

**B.A.** – Arts and Science, University of Omaha, 1998

Communications, Creighton University, 2004

**Masters, Data Science** (in progress)  
Creighton University

#### Time with Firm

Since 2017

#### Certifications/Licenses

Collection Agency Manager

#### Role & Responsibilities

- Oversees production of staff as well as the leadership team for frontline collections
- Determines work procedures, prepares work schedule and expedites workflow
- Reviews policies and procedures for improvements or updates
- Works closely with recruiting team to ensure proper staff levels are being met
- Creates and implements training curricula that meet client standards
- Reviews reports and prepares projections for VP and client
- Bring onboard and terminates employees
- Proposes and implements corrective action monthly for staff performing below expectations
- Stays within payroll budget for department
- Follows and enforces guidelines as defined in State and Federal Laws as well as client and internal procedures
- Creates strategy for staff workload and assigns delinquent accounts to staff for follow up with the consumers.
- Administers performance by providing effective feedback and opportunities for improvement
- Creates and updates spreadsheets used companywide to track performance
- Handles consumer complaints and confidential information



## Alexander Wilson, LL.B., LL.M.

### *Vice President, Legal & Compliance*

#### Areas of Expertise

- Legal documents
- Contract negotiations
- Compliance
- Regulatory affairs
- Employment law
- Litigation matters

#### Time with Firm

Since 2015

Alexander joined the Gatestone team in 2015 and currently oversees the company's Legal & Compliance Department. His extensive expertise enables him to skillfully undertake all of Gatestone's compliance, regulatory affairs, corporate licensing, contract review, and litigation activities. Alexander manages ongoing compliance monitoring with the scope of the company's code of professional conduct, policies, and procedures. He acts as an interface with the audit department to perform periodic compliance audits. Alexander also provides guidance to managers and staff regarding control procedures and testing and assists the firm's leadership to identify compliance risks and in implement plans to monitor and address risks.

#### *Role & Responsibilities*

Alexander provides legal services while ensuring compliance with applicable legislation. He drafts and supports the negotiation of legal and corporate documents including supplier contracts and regulatory and compliance filings and responses. Alexander also provides advice and assistance to the executive team in relation to a wide variety of legal and business matters and provides representation for legal proceedings, agreements, and regulatory compliance matters.

Alexander manages external legal counsel relations and engages in external support for legal proceedings such as contract negotiations, employment law, and litigation matters, as required. He ensures that all policies, by-laws, and documentation are fully compliant under applicable legislation and addresses and identifies internal areas of concern, endeavoring to provide resolution so as to not progress to a legal matter.

Alexander regularly coordinates with department heads and various stakeholders to ensure operational compliance. He is responsible for monitoring the legal spend and appropriate use of legal budget. He assists with the preparation and review of various business documents and communications, such as corporate communications, press releases, advertising, marketing materials, and other documents that impact the business, while assisting with risk management activities to ensure credit and liability risk are mitigated appropriately.





## Dayira Quiel

### Director, Client & Support Services



Dayira Quiel holds more than 15 years of customer support experience. The Client and Support Services team she manages is deeply committed to ensuring a successful outcome for every client. Her purpose is to serve as a key strategic liaison and project manager, overseeing client inquiries through resolution while ensuring client satisfaction including provision of all reporting requirements for the program. Dayira has a wealth of experience across a number of back-office and support services aspects and a thorough knowledge of industry regulations, enabling her to manage procedure development, implementation, and client services for all clients.

### Role & Responsibilities

Dayira provides continuous leadership, training, and professional support to a team of client solutions support representatives. She oversees the administration offices, working closely with the managers to ensure that all employees are compliant with Gatestone's policies. In addition, Dayira leads assigned projects from transition and implementation through to onboarding, including maintenance of projects' documentation.

Dayira's expertise is in preparing materials and remediation plans for client audits and conducting high-level analysis and problem-solving for escalated issues. She establishes metrics and produces reporting to help manage business effectively and in a timely fashion while ensuring that all tasks are completed in a timely fashion for clients and for the operation team internally.

Dayira collaborates and communicates with our clients' internal service desk personnel for incident management, problem management, and remediation to ensure effective implementation of required programming/change management requests from our clients. Her knowledge is instrumental to analyzing data to identify possible gaps in the process, thereby ensuring that all client expectations are met.

### Areas of Expertise

- Call monitoring
- Trend analysis
- Complaint resolution
- Policy development
- Policy implementation

### Time with Firm

Since 2002



## Suzanne Huether

### Director of Human Resources



Suzanne is responsible for overseeing the Human Resources and Recruitment & Corporate Training department functions and supervising the employees. Suzanne manages the administration of employee contracts, on-boarding, employee files, compensation and benefits, recruitment, selection, and training and development. She also ensures company compliance with regulatory and client-based employment standards.

### Role & Responsibilities

Suzanne develops and implements Human Resources strategies and initiatives aligned with the overall business strategy. She manages the recruitment and selection process and bridges management and employee relations by addressing demands, grievances, or other issues.

### Areas of Expertise

- Human Resources
- Updating job requirements and job descriptions.
- Recruiting, testing, and interviewing
- Management counsel
- Orientation and training
- Legal compliance

Suzanne is responsible for the overall development and monitoring of Human Resources strategies, systems, tactics, and procedures across the organization. She supports current and future business needs through the development, engagement, motivation and preservation of human capital and she nurtures a positive working environment.

Suzanne oversees and assesses development needs to apply and monitor training programs. Suzanne is instrumental in ensuring legal compliance through human resource management all while providing the executive team with the support required to make decisions based on Human Resource metrics.

### Education

**B.A.** – Sociology, McMaster University

**Diploma** – Business Administration,  
Algonquin College

### Time with Firm

Since 2002

### Certifications/Licenses

Certified Human Resources Leader  
(CHRL), 2014

Certified Human Resources  
Professional (CHRP), 2012



## Tracy Burks

### Manager, Training & Development

#### Areas of Expertise

- Training program development
- Needs assessments
- Training events
- Coaching
- Communications

#### Time with Firm

Since 2018

#### Certifications/Licenses

Six Sigma Lean Professional, 2019  
Change Management Specialist, 2019  
Corporate Trainer Certified, 2019

Tracy Burks oversees our Training department and develops Gatestone's Call Center training programs to ensure comprehensive instruction on all protocols, Gatestone policies and procedures, and client-specific requirements. Tracy has been directly involved in developing and providing training to our employees since 2018. She is actively involved in a number of industry organizations in order to remain current and knowledgeable on regulations and best practices in Call Center operations and training techniques. Tracy holds her Six Sigma Lean Professional, Corporate Trainer Certified and Change Management Specialist certifications.

#### Role & Responsibilities

Tracy is responsible for obtaining and developing effective training materials, utilizing a variety of media for all Gatestone clients. She oversees the training procedure to ensure that all employees are given the skills they need to be effective. As well, Tracy conducts annual training and development needs assessment while planning and facilitating employee development and training events. She conducts follow-up studies of all completed training to evaluate and measure results and modifies programs, as needed.

Tracy's experience lends itself to the effective training and coaching of managers, supervisors and others involved in employee development efforts. She develops and maintains organizational communications such as intranet bulletin boards and newsletters to ensure employees have knowledge of training and development events and resources.

Tracy exemplifies the desired culture and philosophies of Gatestone and works effectively as a team member with other members of management and the Human Resources staff.





## Chelsea Soulier

*Manager, Human Resources*

### Areas of Expertise

- Regulatory compliance
- Human resources strategies
- Employee development
- Performance appraisals
- Training programs

### Professional Registrations / Affiliations

Society for Human Resource Management

### Time with Firm

Since 2017

Chelsea holds more than seven years of experience managing Human Resources departments and provides employee relations guidance and leadership and is responsible for talent acquisition, the administration of employee contracts, on-boarding, employee files, benefits. She also ensures compliance with regulatory and client-based employment standards. Chelsea is a member of the Society for Human Resource Management.

### Role and Responsibilities

Chelsea develops and implements Human Resources strategies and initiatives aligned with the overall business strategy. She bridges management and employee relations by addressing demands, grievances or other issues and manages the recruitment and selection process.

Chelsea is responsible for the overall development and monitoring of Human Resources strategies, systems, tactics and procedures across the organization. She supports current and future business needs through the development, engagement, motivation and preservation of human capital and nurtures a positive working environment.

Chelsea oversees and manages a performance appraisal system that drives high performance and maintains the pay plan and benefits program. As well, she assesses training needs to apply and monitor training programs. Chelsea is instrumental with ensuring legal compliance through human resource management all while providing the executive team with the support required to make decisions based on Human Resource metrics.



## 2. Solution Approach

## 2. SOLUTION APPROACH

### 1. UNDERSTANDING OF THE PROJECT REQUIREMENTS

Gatestone understands that this request for proposal (RFP) is intended to provide additional call center support services to the State of Nebraska for the ACCESSNebraska program for a contract period of three (3) years with the option to for three (3) renewals of one year each. The additional customer service resources being provided under this contract would consist of receiving inbound calls and/or performing back office processing services.

The contractor selected to provide these services will provide status updates for service requests and will assist with completing change requests and applications, which may require outbound calling and some back-office processing services. Outreach services may include appointment setting as well as processing returned mail, data entry and lookup, and document processing. We understand that up to 10% of calls may require fluency in both English and Spanish and that 10% or more agents must be fluent in both at any given time. Calls will be recorded and distributed to DHHS on a daily basis.

Inbound calls will be routed to the contractor's call center weekdays from 8:00 am-6:00 pm Central Time and must be answered with a maximum average speed to answer of five minutes or less. Data and information received as part of the service will be stored and processed in a secure manner and unauthorized individuals will not be able to access it. Personal Health Information (PHI) and Personal Identifying Information (PII) will be protected at all times in accordance with Federal law.

The contractor will manage staffing and training, and will use a "train the trainer" approach to ensure that all staff members follow all DHHS procedures and any new processes that may be required. Each month, at least five (5) calls per agent will be monitored for quality, and scores will be made available for DHHS staff.

Reporting will be maintained per the RFP requirements on Page 31 of the RFP, *Item 2 Reporting Requirements*.

### 2. PROPOSED DEVELOPMENT APPROACH

Gatestone has a robust implementation and project management process specifically tailored to provide a smooth implementation of the State's ACCESSNebraska Call Center Support program. Our implementation process is administrated by a customized Project Implementation Plan which provides an outline, coordinates, and details of all program task deliverables, project milestones/dates, and resource estimates to demonstrate our readiness for the project.

Gatestone's Project Managers bring a breadth and depth of relevant project management experience as a result of their long tenure with the company. Our Project Implementation Plan for the State will be closely managed and coordinated separately by an assigned, dedicated Project Manager who utilizes a standard template, which has been developed based on a multitude of similar size and scope program implementations, and will be further customized to include the State's specific program requirements. The Project Manager is responsible for maintaining, updating, and distributing the plan to the members of the project team and also assesses potential risks and selects alternative courses of action to attain the stated goals of the program.



Throughout the project implementation process, the Project Manager closely monitors timelines and solution flexibility and incorporates adherence during implementation of the State's program goals. Gatestone already has the physical space and infrastructure in place and can immediately onboard the State's program.

We have nearly 100 years in business, implementing similar size and scope projects for governments, large institutions, and an array of Fortune 500 companies. The Project Implementation Plan for the project will prove to be a key part of the program's launch and ongoing provision of service and will be used to measure and track progress, define responsibilities, and chart milestones to ensure implementation timelines are met. It will provide a dynamic workflow chart that will be continually updated based on new and revised project information with all major milestones identified and individual responsibilities assigned. Regularly scheduled meetings will be held with all respective departments involved with the State's program to outline the strategy for implementation of the project. This is a tested and methodical approach which Gatestone uses for all of our new initiatives and it has a proven formula that works.

Your assigned Project Manager has access to planning tools and other software to document, manage, control, monitor and deliver through to completion of the project within the established timelines.

Our Project Implementation Plans typically includes 10 basic steps as follow:

- **Step 1:** Identify the project and explain the project plan to key stakeholders, discussing all key components
- **Step 2:** Identify and meet with stakeholders and identified department members to define roles and responsibilities
- **Step 3:** Hold a kickoff meeting to initiate the planning process, define and prioritize the project goals and deliverable
- **Step 4:** Define the project scope statement, tasks, and deliverables
- **Step 5:** Develop the project scope baseline, build project teams, and assign resources
- **Step 6:** Develop the Project Implementation Plan with schedules and cost baselines and present to stakeholders and department members
- **Step 7:** Create baseline management plans
- **Step 8:** Develop a staffing plan
- **Step 9:** Gather feedback, identify issues, and complete a Quality and Risk Assessment
- **Step 10:** Adjust Project Plan accordingly

The status of the project is communicated regularly to all key decision makers so they are aware of the continued progress along with any potential risks causing the project to hinder/delay the completion of tasks and deliverables. Gatestone's ticketing system automatically updates all parties by email of any changes and or advancements in planning tasks and objectives.

### 3. TECHNICAL CONSIDERATIONS

Our incoming capacity is in the hundreds of thousands of calls per day. With the addition of IVR and other technologies and channels such as chat, the capacity can be measured in the millions.

Gatestone has the available skilled operator base and infrastructure to be able to handle large call volumes. Our American call centers have the capacity to accommodate hundreds of agents, with additional capacity available in Canada and other countries. We have successfully on-boarded mid to large inbound and outbound contact and call center services for a wide range of clients over the last few years.

Gatestone's standard practice is to overstaff our workforce to account for any unexpected absence such as illness, vacation, or emergency circumstance, as well as to provide for a short-notice ramp-up as any assignment under this contract would necessarily be. Planned work schedules for all agents are 90% capacity in order to cover these situations and any potential call volume surges or seasonal increases. We are able to allocate any required FTE per any portfolio requirements within 24 hours' notice and complete client-specific training of reallocated staff for active operations within 72 hours' notice. We maintain a pool of cross-trained agents who are available for rapid allocation to any portfolio that requires additional staffing.

#### Automatic call distributor

The contact center platform supports skill-based routing that can be prioritized based on experience, function / role or other skills (such as language).

#### Call recording systems

Gatestone utilizes various call center services that each support 100% call recording with configurable retention period for each call center individually. Recordings can be searched using various metadata such as phone number, account, agent, time/date, and other factors and can be streamed or downloaded with the applicable permissions.

#### Technical architecture

Gatestone uses hosted cloud-based call center solutions that provide wide-ranging features (ACD, IVR, call and screen recording, compliance controls, APIs for integrations, etc.) and are extremely scalable and stable. These CCaaS (Contact Center as a Service) solutions use multiple carriers and run in multiple IaaS (Infrastructure as a Service) locations such as AWS (Amazon Web Services) and GCP (Google Cloud Platform), each of which has multiple availability zones (physical data centers).

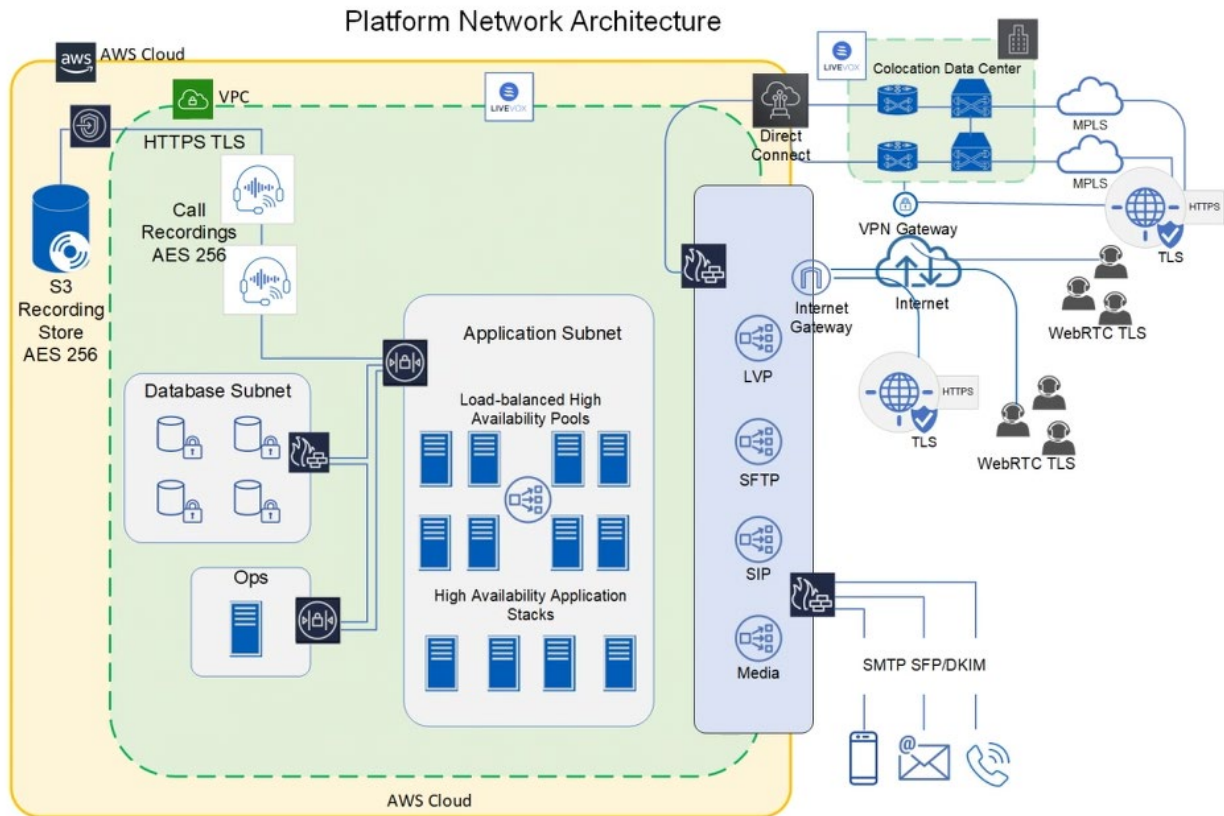
Gatestone's data connectivity can expand to any capacity and has no limitation. Presently, we are using 2 X 20 MB SIP connections and 17 PRI's converted to SIP directly at the SIP provider. These can be expanded quickly, as required by Nebraska, to any capacity. Gatestone uses an Avaya phone switch for this capability.

Gatestone uses VMWare VDI's to replicate our servers to alternate offices, VEEAM software to backup to network attached storage, and Amazon storage to house archived data for recovery.

All users will use the latest Windows operating system machines with the updated patches and firmware updates applied on them. Users will also be assigned a soft token (multi-factor authentication) accessible

via their cell phone or laptop to be used when accessing Gatestone systems. On the back end Gatestone has a back end of Windows server farms with an active directory.

On the following page is a representation of the contact center platform that is hosted on AWS.



## 4. DETAILED PROJECT WORK PLAN

Gatestone’s transition methodology and project plan includes a robust project management process specifically tailored to provide a smooth transition and implementation of the ACCESSNebraska program. We have almost 100 years in business, implementing similar size and scope projects for governments, large institutions, and Fortune 500 companies. Our project management approach is led by our dedicated onboarding team and includes collaboration from all functional teams including program management, operations, human resources, workforce management, reporting and analytics, training and development, information technology, security, change management, finance, quality and compliance, legal and regulatory, risk management, and client solutions.

Our implementation process is tightly managed and provides an outline, coordinates, and details of all task deliverables, project milestones/dates, and resource estimates to demonstrate readiness for the project. The State’s project implementation will be managed and coordinated separately by an assigned, dedicated Project Manager as described previously. Throughout the transition and implementation process, the Project Manager closely monitors timelines, solution flexibility, and incorporates adherence during transition to achieve program goals. Gatestone has the physical space and infrastructure ready to immediately onboard ACCESSNebraska’s program on short notice.

We have identified the following broad deliverables which will fall into the scope of onboarding activities for the ACCESSNebraska program. We anticipate that a broad outline of the plan will be developed prior to a needed deployment in order to facilitate quick implementation.

- Kickoff and review of implementation plan
- Finalize technology and site requirements
- Finalize staffing model
- Reassign staff
- Define and conduct implementation work streams
- Set up technology as needed
- Perform initial user testing
- Modify plans and connectivity based on test results
- Train and test staff
- Define reporting requirements

Many of these tasks will be performed simultaneously for the sake of time. The status of the project will be communicated regularly to the State and Gatestone's project team so they are aware of the continued progress along with any potential risks causing the project to hinder/delay the completion of tasks and deliverables.

Gatestone provides oral and written English and Spanish service at all our facilities in the United States, with a minimum of 20-30% (based on location) contact personnel providing bilingual service at each site. Additionally, Gatestone's diverse pool of agents provide additional language service in; Cantonese, Mandarin, French, Punjabi, Tagalog, German, Italian, Portuguese, Russian, Arabic, Farsi, Tamil, Korean, and Vietnamese and 40+ other languages.

### Program Management Methodology

As a matter of course, Gatestone follows a structured Program Management methodology, which is all the more important on critical initiatives such as the ACCESSNebraska. Following this methodology strengthens the relationship and program integrity and provides structure and confidence, incorporating the 4 foundations of **Planning and Decision Making**, **Organizing**, **Leading**, and **Controlling**. These are the principles that drive our Overall Relationship Management Plan (ORMP). Gatestone's core management team has created the ORMP to guide the company through the term of the contract. It is designed to manage and continuously monitor all aspects of the project for compliance and to maintain our obligations as a supplier to the State. This approach allows us to move with speed and clarity, both of which are of great importance to the State.

### Continuous Improvement and Innovation

The ORMP enables the project team to work with all stakeholders so that all parties are aligned and are committed to continuous relationship improvement. The ORMP is designed to utilize open and transparent lines of communication that results in continuous improvement.





## **Overall Approach to Managing Ongoing Relations with the State.**

The ORMP is constructed to consider and confirm the following;

- **Timelines:** The ORMP defines the overall project, including task assignments, and subsequently directs all relationships according to the operating guiding principles.
- **Evolution:** The ORMP is designed to recognize that the Project's governance requirements will evolve from award through onboarding to ongoing operations. The ORMP lays out how Gatestone will work collaboratively with the State to facilitate ongoing contract management and the oversight of deliverables.
- **Objective:** The Plan is developed to successfully coordinate and manage ongoing deliverables associated with the Contract
- **Communications:** The ORMP communications component creates a strong communications process between Gatestone and the State's operations and project teams

## **Key Components and Guiding Principles**

The ORMP is guided by the following key components:

- An overarching focus on effective and efficient service delivery and on client satisfaction, reflected in the performance objectives
- A responsive and flexible management style that fosters respect for both Gatestone and the State's teams' value and the expertise they bring to support the mandate
- The continuous development of agents and leaders in support of their front-line responsibilities
- Demonstrated leadership, evidenced by the core team and its willingness to improve processes and performance by introducing innovative ideas for discussion, agreement, contract amendment and implementation, resolving risks and issues as they arise utilizing the agreed to risk management plan.

## **Ongoing Operations Governance and Relationships Management**

- **Decision making and escalation:** The ORMP sets out the governance (decision-making and escalation) model and relationships management that will be in effect during the ongoing operations phase of the contract. This includes the process for adding new project elements and the change management process.
- **The ORMP governance model** effectively manages current and evolving requirements from the initial contract award through on-boarding to ongoing operations. Gatestone's role within the project governance is to provide a decision-making framework that is logical, robust, and repeatable to govern in lockstep with the State to ensure the delivery of the required outcomes, value for money, and protection of the State's investments. This will enable success by implementing processes and procedures that meet the State's expectations and requirements for this contract. This is designed to enhance our contract management daily activities and facilitate the oversight of deliverables of our mutual goal to provide the required quality of service based on sound management principles.
- **Project Structure, Management, and Governance:** The management and governance principles of this contract are defined by the following concepts:
  - **Stewardship:** activities and processes that safeguard material assets, knowledge, and data repositories and protect them against losses, misuse, and waste



- **Transparency:** measurable outcomes-based results, performance metrics, and reporting
- **Efficiency/timeliness:** accomplishment of or ability to accomplish a job with a minimal expenditure of time and effort
- **Flexibility:** service delivery that demonstrates innovation with a focus on flexibility to adapt to multi-layered change and promote continual service improvement
- **Communication:** implementation of a strong communications model in order to foster an effective working relationship that will help ensure overall success.

## 5. DELIVERABLES AND DUE DATES.

The Gantt chart that follows details the project schedule as currently envisioned. Gatestone builds our project schedules to be flexible, and we will be happy to coordinate with ACCESSNebraska staff members in order to ensure that the final schedule works for everyone.

RFP - Access Nebraska

ID	Task Mode	Task Name	Duration	Start	Finish
1		<b>Preliminary Project Start-up Plan</b>	<b>46 days</b>	<b>Mon 1/23/23</b>	<b>Mon 3/27/23</b>
2		Milestone - Contract awarded	1 day	Tue 3/1/22	Tue 3/1/22
3		<b>Discovery Phase</b>	<b>1 day</b>	<b>Mon 1/23/23</b>	<b>Mon 1/23/23</b>
4		PBX Design	0.5 days	Mon 1/23/23	Mon 1/23/23
5		PBX Licensing	0.5 days	Mon 1/23/23	Mon 1/23/23
6		Call Recordings Solution	0.5 days	Mon 1/23/23	Mon 1/23/23
7		VoIP Monitoring Solution	0.5 days	Mon 1/23/23	Mon 1/23/23
8		CRM Solution	0.5 days	Mon 1/23/23	Mon 1/23/23
9		<b>Procurement</b>	<b>6 days</b>	<b>Tue 1/24/23</b>	<b>Tue 1/31/23</b>
10		Gather requirements from SOW	1 day	Tue 1/24/23	Tue 1/24/23
11		Gather Quotes from Vendors for SBC	1 day	Wed 1/25/23	Wed 1/25/23
12		Gather Quotes from Vendors for Equipment (PC and Phone)	1 day	Wed 1/25/23	Wed 1/25/23
13		Gather Quotes from Vendors for Data Connectivity (MPLS and Internet)	1 day	Wed 1/25/23	Wed 1/25/23
14		Order and Delivery of SBC	3 days	Fri 1/27/23	Tue 1/31/23
15		Order and Delivery of Equipment (PC and Phone)	3 days	Fri 1/27/23	Tue 1/31/23
16		Order and Delivery of Data Connections (MPLS and Internet)	3 days	Fri 1/27/23	Tue 1/31/23
17		<b>CRM Development</b>	<b>7 days</b>	<b>Mon 1/23/23</b>	<b>Wed 2/1/23</b>
18		CRM Design	1 day	Mon 1/23/23	Tue 1/24/23
19		CRM Build (Frontend and Backend)	5 days	Tue 1/24/23	Tue 1/31/23
20		CRM Testing and Debugging	1 day	Tue 1/31/23	Wed 2/1/23
21		Milestone - CRM Development Complete	0 days	Wed 2/1/23	Wed 2/1/23

Critical		Finish-only		Manual Summary	
Critical Split		Duration-only		Project Summary	
Critical Progress		Baseline		External Tasks	
Task		Baseline Split		External Milestone	
Split		Baseline Milestone		Inactive Task	
Task Progress		Milestone		Inactive Milestone	
Manual Task		Summary Progress		Inactive Summary	
Start-only		Summary		Deadline	

RFP - Access Nebraska

ID	Task Mode	Task Name	Duration	Start	Finish
22		<b>Facility Setup</b>	<b>9.5 days</b>	<b>Tue 1/24/23</b>	<b>Mon 2/6/23</b>
23		Identify operations floor plan for production and training	0.5 days	Tue 1/24/23	Tue 1/24/23
24		Setup operations and training space & branding	2 days	Tue 1/24/23	Thu 1/26/23
25		LAN Network Setup Complete in Facility	2 days	Wed 2/1/23	Thu 2/2/23
26		Workstation Image Design and Testing	2 days	Wed 2/1/23	Fri 2/3/23
27		Workstation Setup and Imaging Complete in Facility	1 day	Fri 2/3/23	Mon 2/6/23
28		Milestone - Workstation setup Completed	0 days	Mon 2/6/23	Mon 2/6/23
29		<b>Infrastructure Testing in Facility</b>	<b>1.5 days</b>	<b>Mon 2/6/23</b>	<b>Tue 2/7/23</b>
30		Test Data connectivity for Data between offices and through to ISP	0.5 days	Mon 2/6/23	Mon 2/6/23
31		Test Applications from Workstation	0.5 days	Tue 2/7/23	Tue 2/7/23
32		Test Transferring call from Cloud based CC to desk phone	0.5 days	Tue 2/7/23	Tue 2/7/23
33		<b>Voice Back-End Implementation</b>	<b>8 days</b>	<b>Mon 1/30/23</b>	<b>Wed 2/8/23</b>
34		Design Voice Back-End	1 day	Mon 1/30/23	Mon 1/30/23
35		Assign and configure Rackspace and Network Space	1 day	Mon 1/30/23	Mon 1/30/23
36		Configure Telephony Solution for Deployment	1 day	Wed 2/1/23	Wed 2/1/23
37		Implement rules and COR on Telephony Solution	1 day	Thu 2/2/23	Thu 2/2/23
38		Create and assign extensions	1 day	Fri 2/3/23	Fri 2/3/23
39		Create and add Annoucements, IVR, Music etc.	1 day	Mon 2/6/23	Mon 2/6/23
40		Provision Storage Disks and configure call / screen Recordings	1 day	Tue 2/7/23	Tue 2/7/23
41		Configure and implement VoIP Monitoring	1 day	Wed 2/8/23	Wed 2/8/23
42		<b>Voice Connectivity</b>	<b>7 days</b>	<b>Thu 2/9/23</b>	<b>Fri 2/17/23</b>

Critical		Finish-only		Manual Summary	
Critical Split		Duration-only		Project Summary	
Critical Progress		Baseline		External Tasks	
Task		Baseline Split		External Milestone	
Split		Baseline Milestone		Inactive Task	
Task Progress		Milestone		Inactive Milestone	
Manual Task		Summary Progress		Inactive Summary	
Start-only		Summary		Deadline	

RFP - Access Nebraska

ID	Task Mode	Task Name	Duration	Start	Finish
43		Discovery - validate requirements and design	2 days	Thu 2/9/23	Fri 2/10/23
44		Build placeholder services	1 day	Mon 2/13/23	Mon 2/13/23
45		Request Local Call-Back Numbers	2 days	Tue 2/14/23	Wed 2/15/23
46		Ensure transfer TFN calls to DID's	1 day	Thu 2/16/23	Thu 2/16/23
47		Build Call Center and Recordings as per Nebraska's Retention Policies	2 days	Mon 2/13/23	Tue 2/14/23
48		Call Center UAT	1 day	Fri 2/17/23	Fri 2/17/23
49		<b>Onboard Core Team</b>	<b>11 days</b>	<b>Mon 1/23/23</b>	<b>Mon 2/6/23</b>
50		Client Solutions	1 day	Wed 1/25/23	Wed 1/25/23
51		Project Manager	1 day	Mon 1/23/23	Mon 1/23/23
52		Call Centre Supervisor	1 day	Tue 1/24/23	Tue 1/24/23
53		Technical Lead	1 day	Tue 1/24/23	Tue 1/24/23
54		Quality Analyst	1 day	Tue 1/24/23	Tue 1/24/23
55		Reporting and Analytics	1 day	Tue 1/24/23	Tue 1/24/23
56		Training Specialist	1 day	Mon 1/23/23	Mon 1/23/23
57		Agents	10 days	Mon 1/23/23	Fri 2/3/23
58		Develop Organizational Chart for Access Nebraska Project	0.5 days	Mon 2/6/23	Mon 2/6/23
59		Describe the responsibilities and commitments for key positions	0.5 days	Mon 2/6/23	Mon 2/6/23
60		<b>Modify Management Plans</b>	<b>7 days</b>	<b>Tue 1/24/23</b>	<b>Wed 2/1/23</b>
61		Performance Management Plan	3 days	Wed 1/25/23	Fri 1/27/23
62		Disaster Recovery Plan	3 days	Wed 1/25/23	Fri 1/27/23
63		Privacy Management Plan	1 day	Wed 1/25/23	Wed 1/25/23

Critical		Finish-only		Manual Summary	
Critical Split		Duration-only		Project Summary	
Critical Progress		Baseline		External Tasks	
Task		Baseline Split		External Milestone	
Split		Baseline Milestone		Inactive Task	
Task Progress		Milestone		Inactive Milestone	
Manual Task		Summary Progress		Inactive Summary	
Start-only		Summary		Deadline	

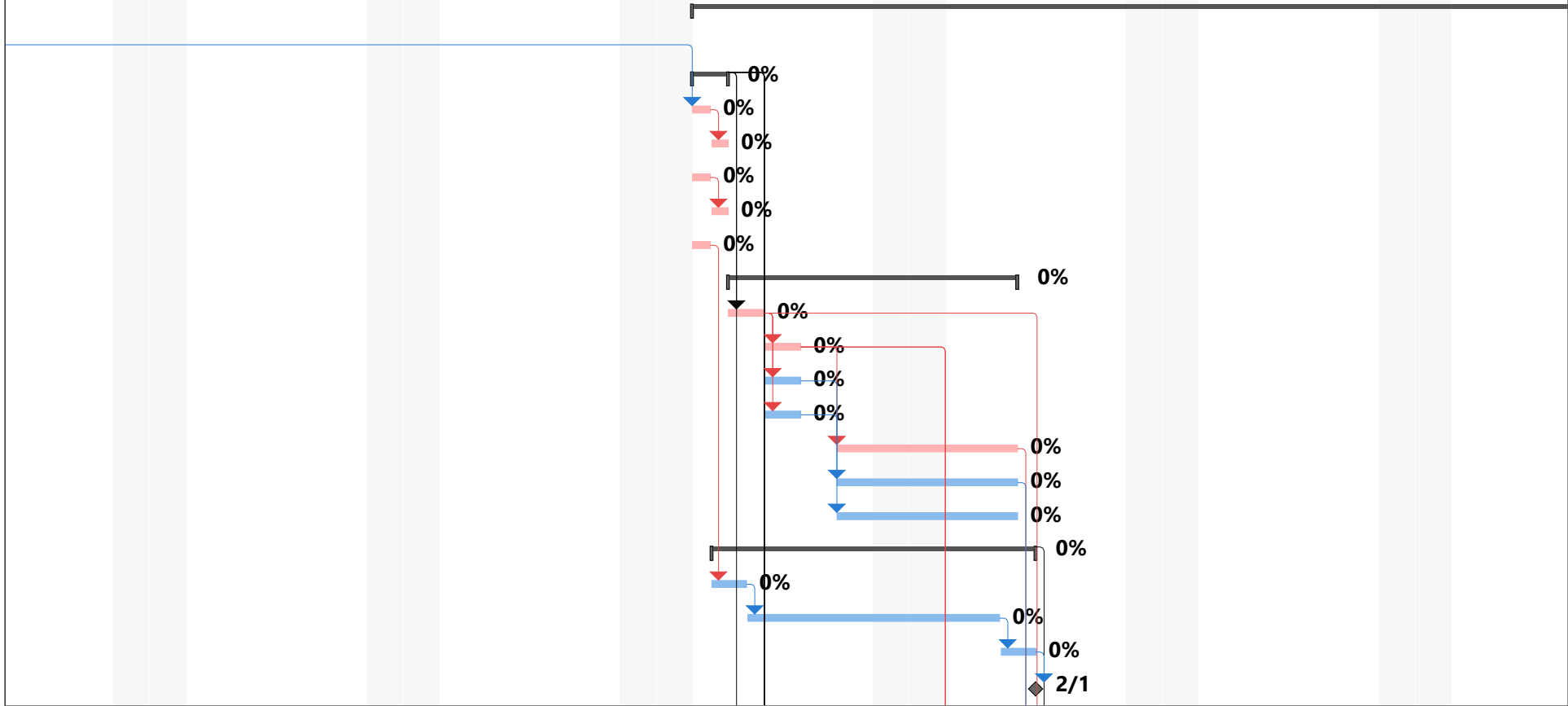
RFP - Access Nebraska

ID	Task Mode	Task Name	Duration	Start	Finish
64		Review Training Plan and Curriculum (from Government of Nebraska)	2 days	Tue 1/24/23	Wed 1/25/23
65		Develop manuals/TEQ knowledgebase with program processes and methodologies	2 days	Mon 1/30/23	Tue 1/31/23
66		Deliver Training Plan to Nebraska	1 day	Wed 2/1/23	Wed 2/1/23
67		<b>Training</b>	<b>25 days</b>	<b>Mon 2/20/23</b>	<b>Fri 3/24/23</b>
68		Train the Trainer	10 days	Mon 2/20/23	Fri 3/3/23
69		Agent training	10 days	Mon 3/6/23	Fri 3/17/23
70		Nesting and Feedback	5 days	Mon 3/20/23	Fri 3/24/23
71		Cutover to Production (Go Live)	0 days	Mon 3/27/23	Mon 3/27/23

Critical		Finish-only		Manual Summary	
Critical Split		Duration-only		Project Summary	
Critical Progress		Baseline		External Tasks	
Task		Baseline Split		External Milestone	
Split		Baseline Milestone		Inactive Task	
Task Progress		Milestone		Inactive Milestone	
Manual Task		Summary Progress		Inactive Summary	
Start-only		Summary		Deadline	

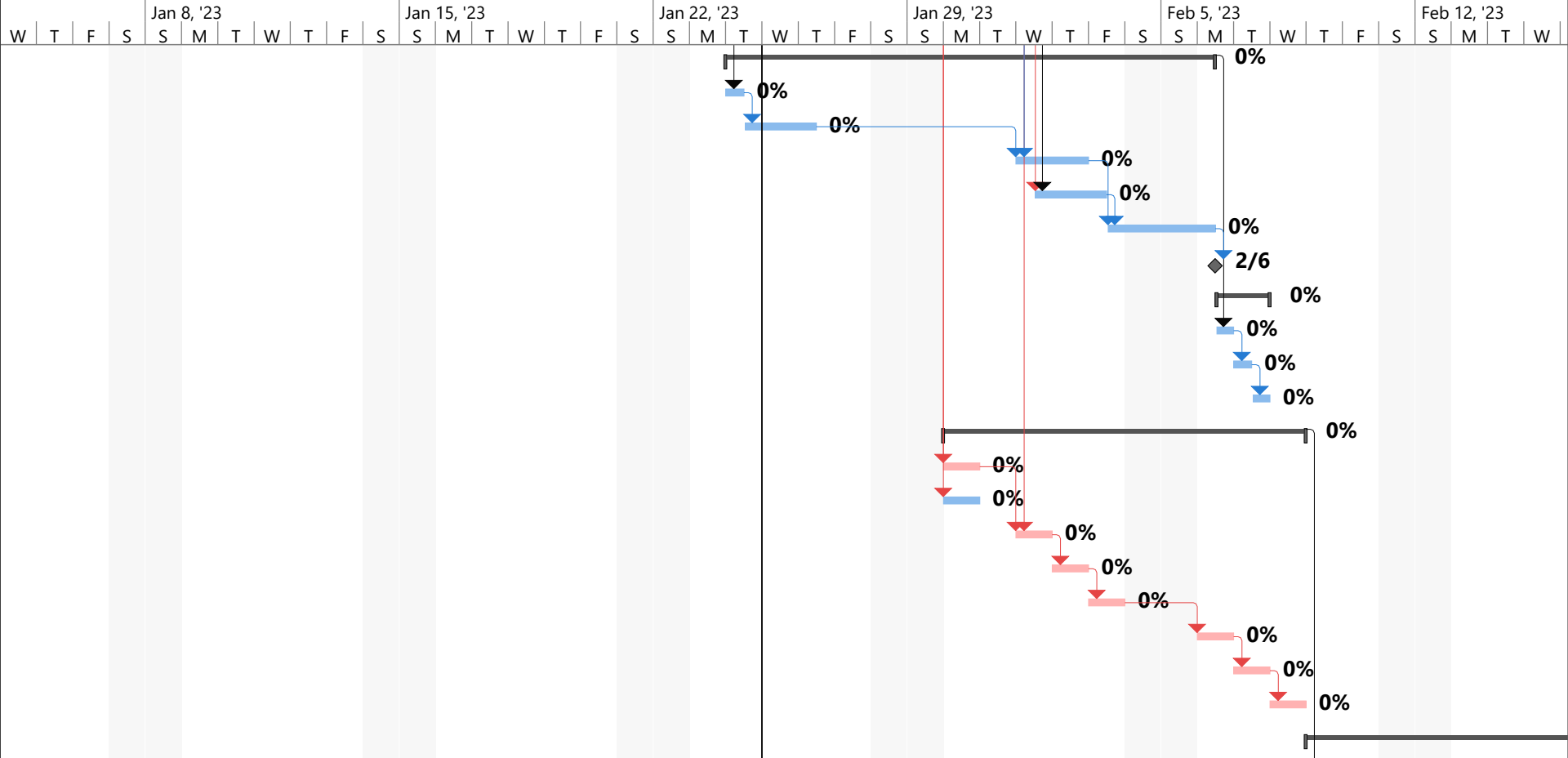
RFP - Access Nebraska

W T F S Jan 8, '23 S M T W T F S Jan 15, '23 S M T W T F S Jan 22, '23 S M T W T F S Jan 29, '23 S M T W T F S Feb 5, '23 S M T W T F S Feb 12, '23 S M T W



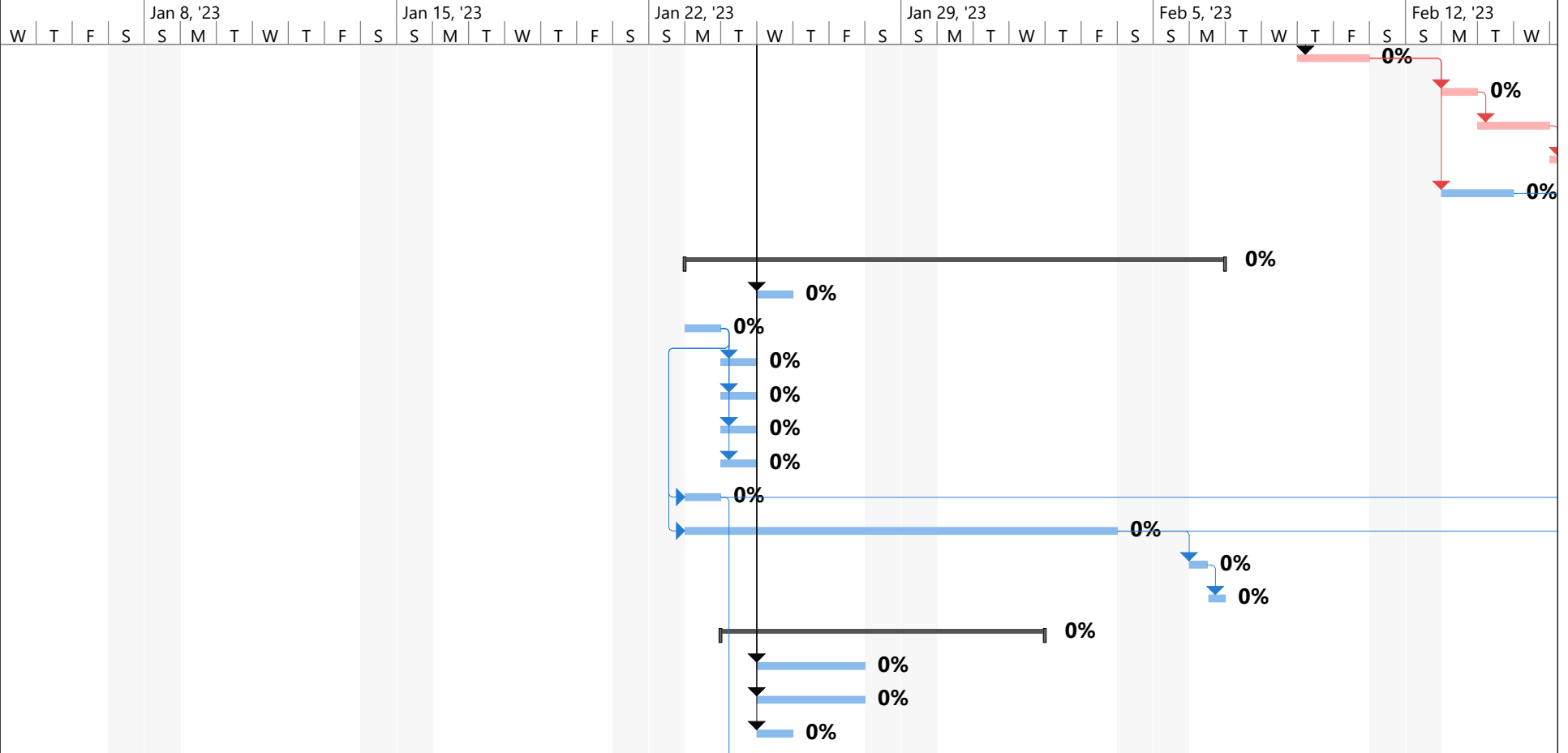
Critical		Finish-only		Manual Summary	
Critical Split		Duration-only		Project Summary	
Critical Progress		Baseline		External Tasks	
Task		Baseline Split		External Milestone	
Split		Baseline Milestone		Inactive Task	
Task Progress		Milestone		Inactive Milestone	
Manual Task		Summary Progress		Inactive Summary	
Start-only		Summary		Deadline	

# RFP - Access Nebraska



Critical		Finish-only		Manual Summary	
Critical Split		Duration-only		Project Summary	
Critical Progress		Baseline		External Tasks	
Task		Baseline Split		External Milestone	
Split		Baseline Milestone		Inactive Task	
Task Progress		Milestone		Inactive Milestone	
Manual Task		Summary Progress		Inactive Summary	
Start-only		Summary		Deadline	

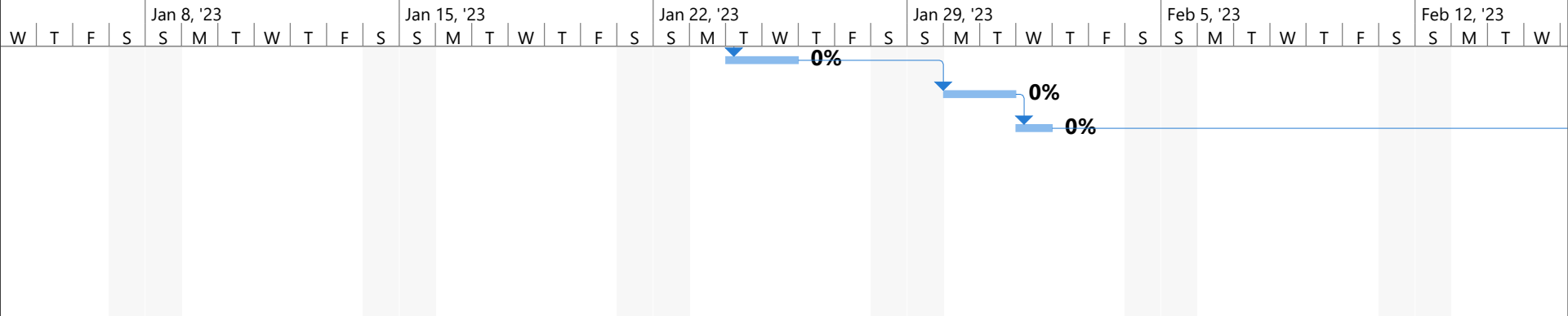
RFP - Access Nebraska



Critical		Finish-only		Manual Summary	
Critical Split		Duration-only		Project Summary	
Critical Progress		Baseline		External Tasks	
Task		Baseline Split		External Milestone	
Split		Baseline Milestone		Inactive Task	
Task Progress		Milestone		Inactive Milestone	
Manual Task		Summary Progress		Inactive Summary	
Start-only		Summary		Deadline	

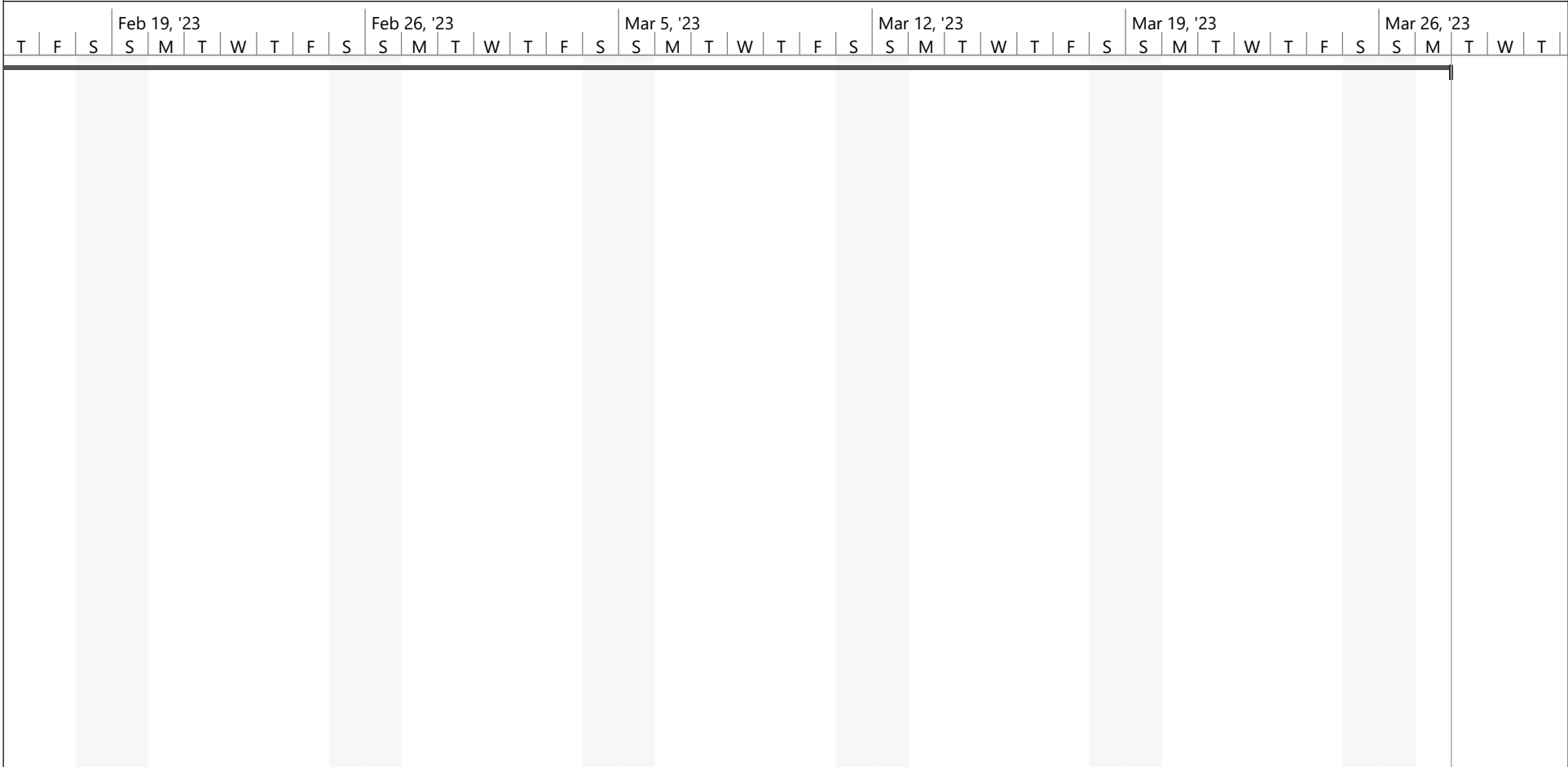


RFP - Access Nebraska



Critical		Finish-only		Manual Summary	
Critical Split		Duration-only		Project Summary	
Critical Progress		Baseline		External Tasks	
Task		Baseline Split		External Milestone	
Split		Baseline Milestone		Inactive Task	
Task Progress		Milestone		Inactive Milestone	
Manual Task		Summary Progress		Inactive Summary	
Start-only		Summary		Deadline	

RFP - Access Nebraska



Critical		Finish-only		Manual Summary	
Critical Split		Duration-only		Project Summary	
Critical Progress		Baseline		External Tasks	
Task		Baseline Split		External Milestone	
Split		Baseline Milestone		Inactive Task	
Task Progress		Milestone		Inactive Milestone	
Manual Task		Summary Progress		Inactive Summary	
Start-only		Summary		Deadline	

RFP - Access Nebraska

T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T

Feb 19, '23

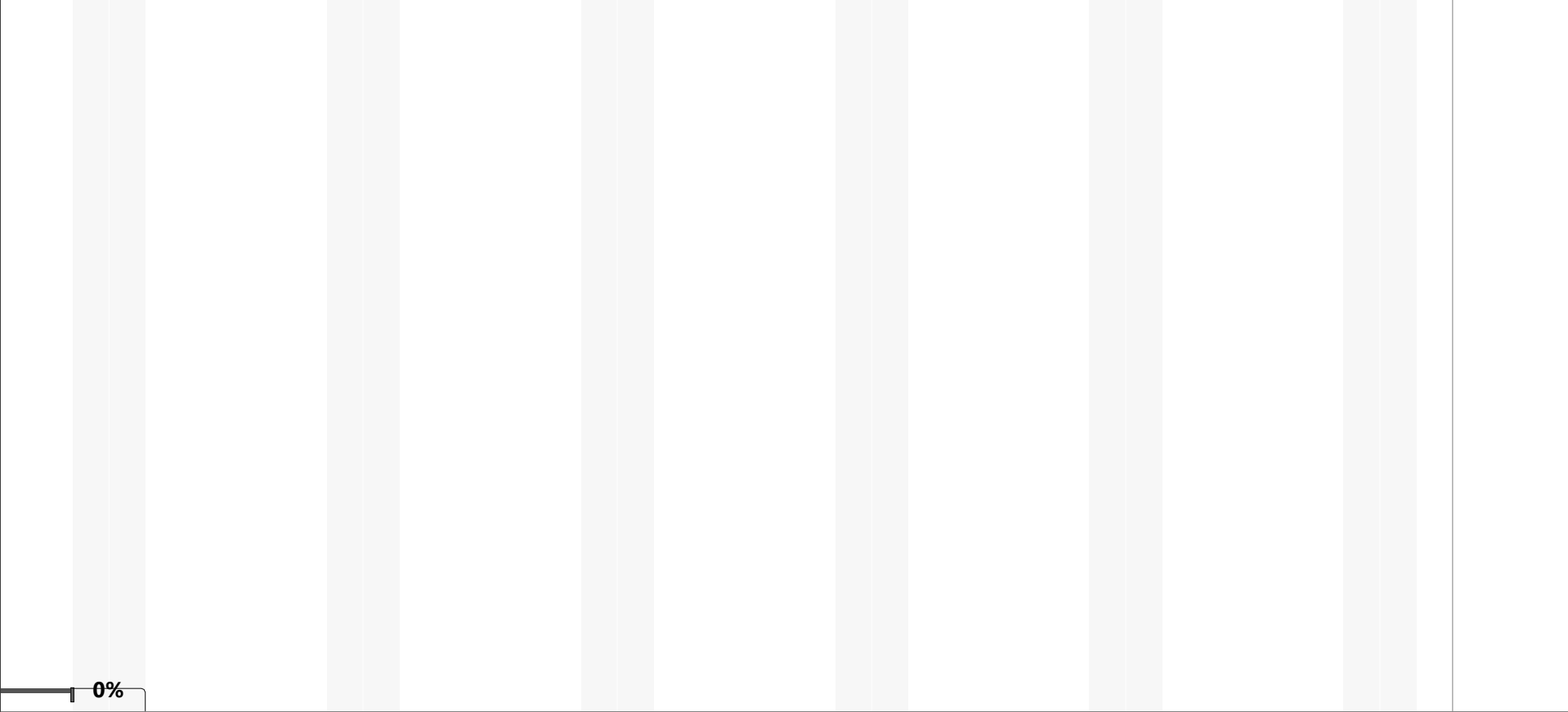
Feb 26, '23

Mar 5, '23

Mar 12, '23

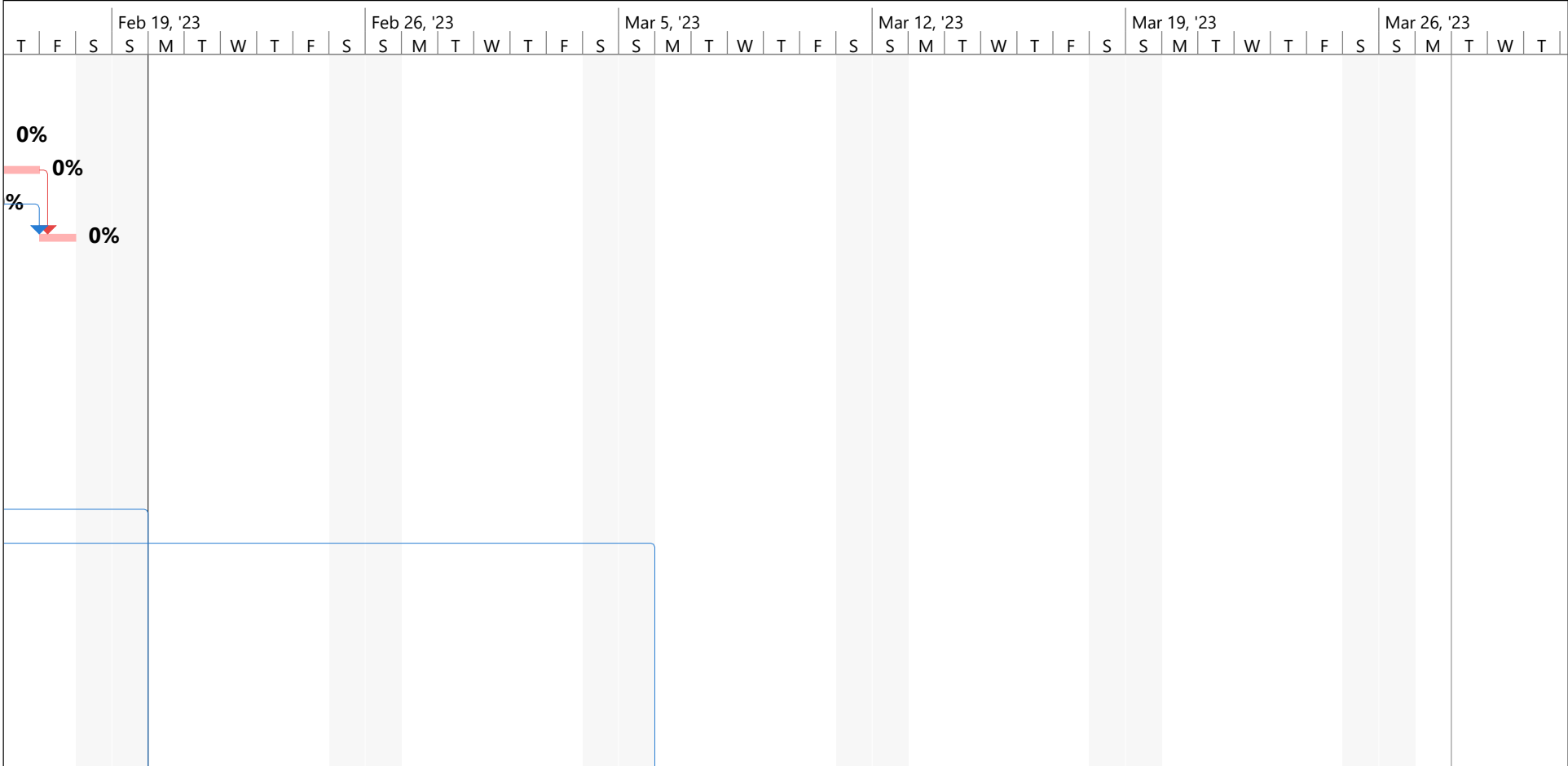
Mar 19, '23

Mar 26, '23

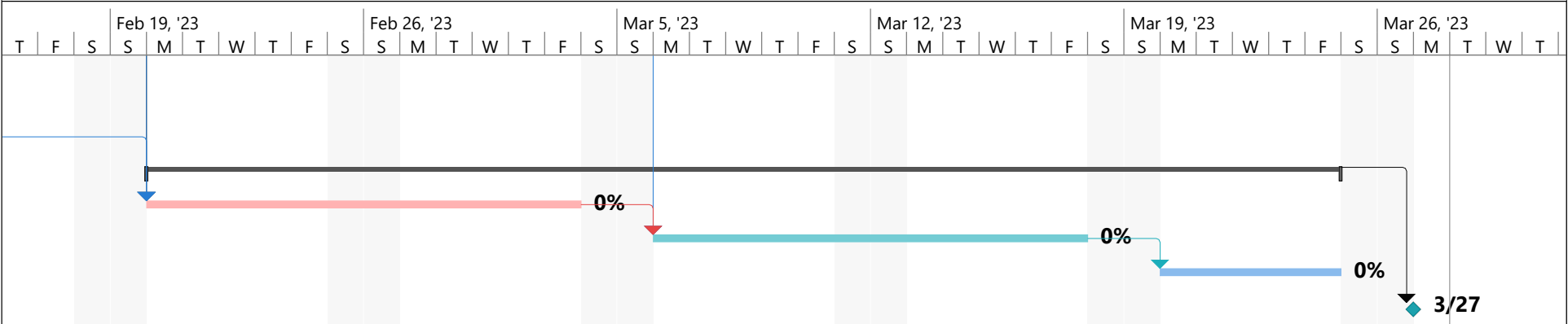


Critical		Finish-only		Manual Summary	
Critical Split		Duration-only		Project Summary	
Critical Progress		Baseline		External Tasks	
Task		Baseline Split		External Milestone	
Split		Baseline Milestone		Inactive Task	
Task Progress		Milestone		Inactive Milestone	
Manual Task		Summary Progress		Inactive Summary	
Start-only		Summary		Deadline	

RFP - Access Nebraska



RFP - Access Nebraska



Critical		Finish-only		Manual Summary	
Critical Split		Duration-only		Project Summary	
Critical Progress		Baseline		External Tasks	
Task		Baseline Split		External Milestone	
Split		Baseline Milestone		Inactive Task	
Task Progress		Milestone		Inactive Milestone	
Manual Task		Summary Progress		Inactive Summary	
Start-only		Summary		Deadline	



### 3. Required Bidder Responses

## ATTACHMENT 3

### REQUIRED BIDDER RESPONSES

	<b>Describe your understanding of the business requirements, including reporting requirements. Describe your approach of how you will accomplish the business and reporting requirements.</b>
1.	<p>Bidder's Response:</p> <p>Gatestone understands that this request for proposal (RFP) is intended to provide additional call center support services to the State of Nebraska for the ACCESSNebraska program for a contract period of three (3) years with the option to for three (3) renewals of one year each. The additional customer service resources being provided under this contract would consist of receiving inbound calls and/or performing back office processing services.</p> <p>The contractor selected to provide these services will provide status updates for service requests and will assist with completing change requests and applications, which may require outbound calling and some back-office processing services. Outreach services may include appointment setting as well as processing returned mail, data entry and lookup, and document processing. We understand that up to 10% of calls may require fluency in both English and Spanish and that 10% or more agents must be fluent in both at any given time. Calls will be recorded and distributed to DHHS on a daily basis.</p> <p>Inbound calls will be routed to the contractor's call center weekdays from 8:00 am-6:00 pm Central Time and must be answered with a maximum average speed to answer of five minutes or less. Data and information received as part of the service will be stored and processed in a secure manner and unauthorized individuals will not be able to access it. Personal Health Information (PHI) and Personal Identifying Information (PII) will be protected at all times in accordance with Federal law.</p> <p>The contractor will manage staffing and training, and will use a "train the trainer" approach to ensure that all staff members follow all DHHS procedures and any new processes that may be required. Each month, at least five (5) calls per agent will be monitored for quality, and scores will be made available for DHHS staff.</p> <p>Reporting will be maintained per the RFP requirements on Page 31 of the RFP, Item 2 Reporting Requirements.</p> <h3>Our Approach to Accomplishing the Project Requirements</h3> <p>Gatestone has been providing comprehensive centralized Business Process Outsourcing (BPO) and call center solutions for a variety of industries such as government, healthcare, financial and insurance services, education, utilities, retail/e-commerce, telecommunications, and logistics. We are currently contracted with more than 30 unique government departments and more than 25 municipalities with our longest public sector client partnership spanning nearly thirty years.</p> <p>Our BPO and call center support services for these clients include a range of services such as</p> <ul style="list-style-type: none"><li>■ General and complex customer service support</li><li>■ Inbound and outbound calling</li><li>■ Frequently Asked Questions (FAQ) support</li><li>■ Application walk-through and upload support</li><li>■ Policy/claims administration</li><li>■ Fraud processing and management</li><li>■ Escalation management</li><li>■ Automated Call Center campaign messaging services</li><li>■ Automated mass text messaging campaigns</li><li>■ Providing systems information</li><li>■ Back office support</li><li>■ Technical help desk support (all tiers)</li><li>■ Appointment scheduling</li><li>■ Customer satisfaction surveys</li></ul> <p>Some of the features of these programs and services include the following:</p> <ul style="list-style-type: none"><li>■ Full automation of Interactive Voice Response and SMS systems including complete customization of recording, dial-back, reporting and archiving in English and Spanish</li></ul>

- System technology to support a variety of omni-channel communication such as live phone calls, Interactive Voice Response, live agent chat, AI chat, e-mail, voice broadcasts, SMS text, social media, and other mobile applications
- Full program customization with support for people with limited technology access or who do not speak English as well as people with hearing, speech, and vision disabilities
- Bilingual and multilingual support, 53 languages spoken in-house with access to a language line for those that fall outside of the languages by Gatestone agents
- Streamlining internal efforts and processes
- Gatestone@Home remote working solution engaging Nebraskans, supported by tools and resources with up-to-date workplace security standards including multi-factor security protection, a cloud-based virtual desktop infrastructure (VDI)
- Flexibility of coverage with 24/7/365 availability
- Agent selection based on a customized proprietary Gatestone Index (GI) Assessment testing tool which identifies candidates most likely to succeed in the State's specific program
- Professional agent training for customer experience and treatment excellence which improves customer satisfaction and protects the State's reputation
- Flexible customized reporting options and 100% call recording

At Gatestone, we have the longest tenured management in the industry. This translates to a tenured pool of existing agents who have the skills and experience required to fulfill the State's program needs. Our large client base and experienced team of agents provide Gatestone with the ability to quickly redirect staff to onboard the State's program, with appropriate additional training, as per the State's program needs.

## Our Call Center Architecture

Across our Call Center sites, Gatestone has the ability and experience to install, configure and implement unique infrastructure based on each client's program requirements. As well, across our Call Center sites, Gatestone has the ability and experience to install, configure and implement unique infrastructure based on each client's program requirements. As well, Gatestone's Information Technology team is well versed and possess the skills required to integrate with any client system, if required. Gatestone's Call Center architecture consists of the following components (at a minimum);

- Interactive Voice Response (IVR)
- Automatic Call Distributor (ACD)/Private Branch Exchange (PBX) Systems
- Soft Phones, IP Desk Phones and Digital Phones
- Call Management System
- Workforce Management System
- Call Recording and Agent Screen Recording System
- Reporting and Analytics System
- Intelligent Call Routing System
- Toll Free Network Service
- Toll Free Network Routing Platform
- TTY Technology to Support Hearing Impaired
- Business Rules Engine for Hours of Operation/Per Site/Per Skill
- Outbound Dialer Notification Capabilities
- Agent, Skill Group, IVR, Call Routing and Toll-Free Reporting
- Gatestone TEQ (Training, Education, Quality) - Agent information exchange platform
- Chat and 'Ask a Question' capabilities

## We are an Experienced Supplier

Some of the Public Sector and corporate brand entities across North America with similar size and scope that Gatestone has experience providing Call Center and Business Process Outsourcing services are shown on the next page:





Gatestone will draw upon the leadership resources, insights and knowledge from these initiatives and apply to the State's program.

One of our greatest strengths is partnering with our clients and maintaining lasting relationships. Many of our clients have been with us for over twenty-five years of uninterrupted service, most notably, a Fortune 500 Institution where we have managed every line of customer care support for this client in the course of our almost forty-year relationship. The ability to retain long-term relationships is based upon our ability to deliver solutions that evolve with the needs of the customers, technology and the regulatory framework they operate within.

For nearly one hundred years, Gatestone has understood that whether working with Public or Private Sector clients, we must constantly build on our capabilities and our past performance. It is this cornerstone philosophy that we will bring to the State, as a matter of course. We are particularly proud of the Business Process Outsourcing, Call Center and Support services we deliver on behalf of Public Sector entities across North America. We have a comprehensive understanding and history of serving the public sector market, and understand the regulations, best practices, and operational processes required to manage this specialized sector.

**Service and Excellence Awards**

Through our diligence in the area of consumer treatment, Gatestone has won several highly prestigious awards service and excellence awards. We are extremely proud of our people and their commitment to providing the most outstanding levels of customer service. We understand that exceptional customer service is a priority for this project and we commit to deliver. Our continuous investment to deliver the best customer experience has earned us numerous performance and excellence awards including;

- **J.D. Power & Associates Customer Satisfaction Award** for exceptional levels of customer treatment
- **Call Center Week Excellence Award for Best Outsource Provider** highlighting best-in-class Call Center sites, comprehensive agent and leadership training, customer-focused quality management and innovation as our key strengths.
- **GTACC Awards for Service Consistency, Contact Center Excellence-Best Over 100 and Giving Back** highlighting our high level of service consistency, best managed center over 100 agents and continuous contributions to our employees and charities.
- **Call Center Week Excellence Award for Best CRM Solution Provider** for excellence in development innovative Call Center solutions.



2.	<p><b>Describe your site security and how you will maintain security for remote workers. Both physical and technology security.</b></p> <p>Bidder's Response:  Gatestone operates within a highly secure environment and treats privacy and confidentiality as our highest priority, which includes the protection of personal data and physical premise security. We hold the highest security designations and continually upgrade our environment and technologies. Our security standards and certifications include: PCI Level 1 certification, ISO27002 certification, SOC1 and SOC2, HIPAA, and NACHA compliance.</p> <p>Gatestone's Business Continuity and Disaster Recovery (BC/DR) Plan provides coverage for all critical assets and is tested on an annual basis. The Chief Security Officer (CSO), network team, and key operational players are involved in the testing process. Annual tests are conducted against service level agreements, recovery time objectives, and recovery point objectives as our guidelines. Any deviation from these objectives are listed as a finding and sent to senior executives for review and guidance. Gatestone's BC/DR capability is based on an 'N+1' concept on all network components and diversified geographical locations. This involves duplicate circuits, internet connections, firewalls, and any other components critical to the process. These are all designed to automatically switch to the alternate device in a failure. The circuits will be designed across diverse geographical areas on diverse circuits. This allows all processes including employee access to continue working if one of our data centers fails.</p> <p>Gatestone exercises an exceptionally high standard of due care with respect to securing information assets, primarily accomplished through security policies, procedures, and practices that are documented, auditable, and enforced. We have implemented and maintain a comprehensive set of security policies and procedures (P&amp;Ps) and have established a solid security awareness program to ensure our employees, sub-contractors and vendors understand them and their importance to operate within applicable laws and regulations. Gatestone uses the ISO 27001 and PCI framework for our security policies, procedures, and practices which we have audited annually by a third party. Gatestone continually monitors our security policies and procedures for compliance and takes immediate action up to termination if anyone is found in non-compliance. Our Physical Security Policy addresses physical security of our facilities, swipe card enabled limits on access to specific areas within our facilities for both employees and visitors, strong firewalls for network protection, workstation hardening, and limits on access to information assets based on need to access.</p> <p>Gatestone will provide remote, virtual office, and teleworkers access to our systems and direct connection to the State of Nebraska out of our Omaha, Nebraska site and, in a BC/DR situation, out of a redundant data center. All remote worker equipment is supplied by Gatestone and they adhere to all the same security policies and procedures that are enforced for onsite office workers including 2 factor authentication, SCCM image enforcement, and role-based access control, all of which is encrypted over IPSEC VPN protocols. The same equipment is used in the office and at home to make security invisible to the employees as it follows them wherever they log in.</p> <p><b><i>Please see the attachments that follow in this section, including our Physical Security Policy, Security Policy, and Work from Home Policy.</i></b></p>
3.	<p><b>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.</b></p> <p>Bidder's Response:  Gatestone provides oral and written English and Spanish service at all our facilities in the United States, with a minimum of 20-30% (depending on location) call center resources providing bilingual service at each site. In addition, Gatestone's diverse pool of agents provide additional language service in Cantonese, Mandarin, French, Punjabi, Tagalog, German, Italian, Portuguese, Russian, Arabic, Farsi, Tamil, Korean, and Vietnamese and more than 40 other languages.</p>
4.	<p><b>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.</b></p> <p>Bidder's Response:</p>

	<p>Gatestone is committed to providing its clients with exceptional HIPAA-compliant services while assuring the safety and protection of all Protected Health Information. Gatestone has been providing support services to the healthcare industry since 1989, and is fully aware and compliant with all relevant laws, statutes and best practices around protected information. Our HIPAA Confidentiality and Systems Usage Breach Policy is designed to outline our commitment to having the physical, network, and process security measures in place and following them to ensure HIPAA Compliance across all our operations. <b>Our HIPAA Policy follows this section.</b></p> <p>Gatestone’s cloud-based, integrated, dialer technology applies rigorous safeguards to ensure safety, security, privacy and regulatory compliance with;</p> <ul style="list-style-type: none"> <li>■ End-to-end data encryption to ensure compliance with HIPAA requirements for handling Protected Health Information (PHI), as well as international data regulations;</li> <li>■ Security framework including NIST, OWASP, ISO27001, SOC2 and PCI-DSS Level 1;</li> <li>■ Administrative, physical, technical, organizational, and documentation controls for securing electronic PHI as required by HIPAA;</li> <li>■ Flexible cloud deployments localized to affiliate country and regulatory requirements.</li> </ul> <p>Gatestone’s HIPAA compliance training is mandatory, as required and is administered upon hire and typically twice annually. Our HIPAA compliance training;</p> <ul style="list-style-type: none"> <li>■ Ensures the confidentiality, integrity, and availability of all PHI that agents create, receive, maintain or transmit (electronically or otherwise);</li> <li>■ Identifies and protects against reasonably anticipated threats to the security or integrity of the information;</li> <li>■ Protects against reasonably anticipated, impermissible uses or disclosures; and</li> <li>■ Ensures compliance by Gatestone’s workforce engaged in the work.</li> </ul> <p>Gatestone is not a covered entity nor a business associate under HIPAA.</p>
5.	<p><b>Describe how you will securely print and mail documents.</b></p> <p>Bidder’s Response:  Gatestone does not permit any printing from home offices. Printing from the office requires a passcard to release secure print jobs. Permissions are role-based. Mailing is done by third-party vendors who have been vetted through our onboarding risk management process. Typically, mail that is intended to be delivered outside of the organization is sent First Class, with traceable delivery required.</p>
6.	<p><b>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.</b></p> <p>Bidder’s Response:  To ensure compliance with the government regulations, Gatestone has established strict operating procedures to ensure the security and confidentiality of the personal consumer information staff is collecting, using, or disclosing as part of the daily routine activity and practices.</p> <p>Gatestone implements and maintains comprehensive (P&amp;Ps) established to fulfill federal, state, and local privacy laws and all client expectations and maintain a high standard of compliance and service. Our P&amp;Ps are incorporated into our mandatory training curriculum to ensure all employees handle confidential personal information in a secure manner. Our security and privacy awareness training program is mandatory for all employees during onboarding and throughout their employment, at both random and scheduled timeframes, as implemented by our Chief Security Officer. Each and every Gatestone employee must undergo this training and complete a test obtaining a pre-determined score to complete the program. Successful completion of the initial and ongoing training is tracked on our proprietary software, <b>GatestoneTEQ</b>. Our policies are posted on our website for public access. A list of our related policies and procedures related to how we properly handle confidential personal information are provided below:</p> <p><b>Gatestone’s Code of Conduct:</b> provides a framework to ensure orderly operations and provide a favorable work environment for all employees.  <b>Compliance Management Policy:</b> sets out expectations for the compliance function to ensure all legal requirements are effectively documented and communicated.  <b>Personal Information Privacy Policy:</b> outlines our commitment to protecting consumer rights and incorporates controls to ensure adherence to privacy laws.</p>

	<p><b>Physical Security Policy:</b> is based on the use of management approved security standards in coordination with the Company Security Officer and the Executive Team.</p> <p><b>Security Policy:</b> provides a framework to maintain a secure networked environment.</p> <p><b>Telecommunications Policy:</b> outlines compliance with federal and state laws regarding telecommunications and dialer practices.</p> <p><b>Complaint Handling Policy:</b> sets out the policies to ensure customer complaints are efficiently and effectively managed.</p> <p><b>Fraud and Abuse Policy:</b> outlines the guidelines for anyone who knows of or suspects fraud, abuse, mismanagement, or violations of laws and regulations.</p> <p><b>Work from Home Policy:</b> provides guidelines/regulations for work from home employee. and works alongside our External Telecommuting Security Standards, Telecommuting Policy and Telecommuting Agreement.</p> <p><b>Internet Usage and Accessibility Policy:</b> outlines guidelines to prevent usage of the internet for unauthorized purposes.</p> <p><b>E-Mail and Encryption Policy:</b> uses encryption technologies at the server level to safeguard sensitive information and ensures data/information is not compromised.</p>
7.	<p><b>Describe your ability to meet the facility requirements for the printing functions?</b></p> <p>Bidder's Response: All printing is done on-site at a secure facility that is encrypted end to end and all print jobs require badge access cards for release. If more printing is required than our facilities are equipped to provide, we have vetted several print vendors through our risk assessment procedure. These include RevSpring, Kubra, and High Cotton, which are able to both print and send mail securely.</p>
8.	<p><b>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.</b></p> <p>Bidder's Response: Gatestone's Workforce Management (WFM) Department consists of long-tenured senior executives who manage forecasting and scheduling utilizing our intelligent workforce planning systems and tools. This team oversees productivity at the individual, departmental, and organizational level and manages staffing for large-scale complex BPO and call center programs.</p> <p><b>Workforce Planning Process</b></p> <p>Gatestone utilizes a comprehensive workforce planning process for scheduling and forecasting. We currently use several scheduling software programs, along with proprietary in-house programs to plan, track and manage the allocation and requirements of staffing resources. Our workforce management software assists with increasing overall efficiency and productivity among employees and works in conjunction with The Gatestone Index (GI) behavioral assessment survey to match the right employee to the right job, allowing operations management to effectively oversee employee operations.</p> <p>Our WFM team has overall responsibility for developing and maintaining staffing requirements. We will assign a WFM Manager to work with the State to develop forecasts and schedules accommodating any fluctuating demands of the contract.</p> <p>Our workforce planning programs provide the following benefits to our clients:</p> <ul style="list-style-type: none"> <li>■ Understanding the speed required for the program and providing reduced time to forecast, schedule, and manage employees maintaining flexibility to meet the State's fluctuating demands</li> <li>■ Decreased turnover and improved employee morale</li> <li>■ Reduced overstaffing costs while improving customer satisfaction</li> <li>■ Improvement of the staffing process, which, in turn, drives increased efficiencies</li> </ul> <p>Gatestone has expertise in multiple methods of forecasting transaction volumes in order to schedule the right number of agents. Most commonly, we utilize a WFM optimization approach which combines monthly forecasted volumes that we receive from our clients with historical data and our many decades of expertise. This understanding, combined with certain specifics of our site's demographics (e.g., the flexibility of agents' schedules, minimum commitment of hours/agent, shrinkage assumptions, full time/part time ratios), allows us to determine the required schedules to handle the call volume and meet required metrics. Once the schedules have been created by the WFM central team, the individual site team will work with the agents to fill the required schedules.</p>

	<p>WFM runs an algorithm to determine the level of efficiency of the schedule as it occurred on the selected basis days and applies results to the new schedule being built. If the level of adherence was low on the selected basis days, the system will build in the additional coverage required to compensate for the anticipated level of non-adherence to the schedule.</p> <p>The team runs future forecasts, three months in advance, based on historical data. They then factor in current trends that have been observed and lock the forecast 45 days out. This gives them the option to make necessary adjustments to the schedules. As we typically manage schedules ranging from 30 hours to 40 hours for full time, we are able to immediately allow for more hours within the day itself and organize it faster when quick scale ups are needed for a few hours or days.</p> <p>As a practice, Gatestone always targets to overstaff to account for attrition, call spikes or any other factors. This also allows us to make quick decisions, maintain flexibility and make micro adjustments on a daily basis due to environmental or technical challenges that can occur when managing day to day operations.</p> <p>Equipment for Staff</p> <p>Gatestone provides the following equipment to all staff:</p> <ul style="list-style-type: none"> <li>■ Laptop: Lenovo Y510P I7-2.4-4700MQ 16GB 1TB SSD with Windows 10</li> <li>■ Laptop: Lenovo E560 ICi5-2.0-4310U 8GB 500GB SSD with Windows 10</li> <li>■ Desktop: Lenovo M72E TINY ICi5-2.90 3470 8GB 500GB with Windows 10</li> <li>■ Logitech keyboard and mouse</li> <li>■ Dell monitors</li> <li>■ Jabra Evolve 20 MS or Jabra Biz 2300 QD Headsets</li> </ul>
<p>9.</p>	<p><b>Describe your quality monitoring processes.</b></p> <p>Bidder's Response:  Gatestone utilizes an industry-leading call recording application to record both voice and screen shots, including call content, call detail records, and screen images for quality purposes and outbound monitoring. For compliance recording, this system records and stores 100% of voice calls. Our recommendation based on industry best practice is 100% screen capture with ten years retention, however recordings and captures are fully configurable as required by ACCESSNebraska.</p> <p>Gatestone establishes remote access to the compliance recording database for clients to enable them to pull any recorded call. Stored call recordings can also be easily requested and retrieved by the Quality Analysts and replayed for quality monitoring, compliance, and dispute management. Our solution allows our Quality Analysts to set predetermined schedules to ensure all agents have the expected number of calls recorded each month and also provides the analysts a tool to track agent scores and progress. This feedback is an excellent opportunity for a coaching session if the agent requires such attention.</p> <p>Gatestone's staff uses <b>Quality Scorecard</b> functionality to review and analyze customer interaction recordings. The agents receive immediate evaluation, scoring, and performance summaries. Gatestone Team Leaders use customized scorecard templates to calibrate scoring among Quality Analysts, create targeted agent training plans and improve coaching sessions. Quality scorecards will be customized with the State to address all the specific program requirements and KPIs that are most important. Gatestone's call recording tool also enables Gatestone to effectively monitor, record, and analyze interactions across several media, including VoIP, web, chat, voice, data, and email. Our clients can also remotely monitor Gatestone representatives via the software. Gatestone's solution allows random monitoring based on customer account number, specific program, skills set, or call type. This monitoring capability allows our clients and Gatestone to evaluate specific programs, identify trends, and refine agent approach and skills. Proactive and targeted monitoring results in improved processes with the result being better quality and higher levels of customer relationships. The solution also allows Gatestone to monitor voice and data in real-time displaying which agents are taking calls.</p> <p>Gatestone's Quality Assurance infrastructure includes a Manager of Quality Assurance (QA) supported by a team of Quality Analysts, a robust Quality Management Plan, GatestoneTEQ knowledgebase platform, LiveVox real-time Quality dashboards and reporting, AI Quality platforms, customized Agent Quality Scorecards, 100% call recording, call calibrations, agent scripting and continuous coaching and side-by-sides with agents. Our Quality Analysts document trends, including customer issues and agent performance, and assist in determining the root cause analysis at the site level. The primary role of this</p>

	<p>position is to define, measure, analyze, and identify key areas of opportunity. Through regression analysis, correlation analysis, and root cause indicators, our Quality Analysts are able to provide an in-depth understanding and a suggestion of targets to increase quality performance and the achievement of goals.</p> <p>These tools, systems and processes all work together to ensure the highest quality of service is consistently delivered.</p> <p>Gatestone's quality monitoring for ACCESSNebraska will include (customized as needed):</p> <ul style="list-style-type: none"> <li>■ 100% call recording to allow for compliance and quality of not just voice, but other aspects of the customer interaction such as e-mail or live chat</li> <li>■ Tools to build customized customer satisfaction surveys</li> <li>■ Random and scheduled call monitoring</li> <li>■ Call calibrations</li> <li>■ 98% scorecard compliance (agent and site level)</li> <li>■ Secure online access provided to the client</li> <li>■ Agent scorecard utilization with a minimum of eight scorecard evaluations per agent per month</li> <li>■ Immediate remediation, training and coaching for each agent where deficiencies are identified</li> <li>■ Root-cause analysis to drive continuous improvement</li> <li>■ Scorecard audit customized for project KPIs</li> <li>■ Recording of all calls with ability to customize based on quality triggers such as; number of holds, transfers, short calls etc.</li> </ul> <p>We have found that tracking procedural adherence is the best way to ensure quality. Our Quality Assurance team will hold the agents to a predetermined goal. Quality Assurance scores lower than this score will receive intensive additional coaching, in the form of written feedback and evaluation scoring, and re-training to correct any issues. If the issue(s) continue, corrective action will commence, and the employee could face remedial action up to and including termination.</p>
<p>10.</p>	<p><b>Describe your ability to meet the timelines established in this RFP for reporting and quality monitoring.</b></p> <p>Bidder's Response:</p> <p>Gatestone confirms our ability to meet all timelines as established in the RFP. Gatestone is already an experienced provider of these call center-related services to a number of Government departments and related entities, and have onboarded all of the programs within the scheduled timeframes, while meeting and exceeding all KPI's. Throughout the project implementation process, the Project Manager closely monitors timelines, solution flexibility, and incorporates adherence during implementation of the State's program goals. Gatestone has the physical space and infrastructure already in place to immediately onboard the State's program. Our reporting and quality monitoring processes are continually in place and can be implemented very quickly for any new programs we bring on.</p> <p>For similar size and scope programs, Gatestone would estimate 30-45 days to set up and launch. We launched a program for a leading Fortune 500 brand with hundreds of locations in one week, when we were approached during the height of the COVID pandemic when their contact center vendor was unable to get people in a work from home environment quickly and was forced to shut down leaving customer calls unanswered and service in disarray.</p> <p>Gatestone is a technology-driven, agile organization that offers the capacity to be flexible, and the ability to make quick adaptations to changes in the environment. We provide our clients a dedicated team of operational and support staff that is responsive, adaptable, and always available. Our program effectiveness and success are viewed on a holistic basis and embrace several factors that include meeting and exceeding program timelines (such as those for onboarding, new program introduction, hiring for ramps etc.), program KPI's (including hours &amp; attrition), quality scores, maintaining uptime and business continuity, ensuring client satisfaction with reporting, effective internal and client communications on the program, continuous program improvement (via operations, our data analytics department, and technology enhancement), and ultimately the satisfaction of the client and their consumers on the work we perform for them. The ability to adapt quickly is essential in providing services to a contract like this one, where that need is an essential requirement. We run our operations in an open and collaborative manner, where our clients view our teams as an extension of their own.</p>



	<p>Our success via our performance and flexibility has led us to maintaining the longest average client tenure in the industry, averaging more than 25 years, and providing continuous service for our longest customer for more than 60 years.</p>
11.	<p><b>Describe your maximum call capacity and the timeframe required to increase call capacity.</b></p> <p>Bidder's Response:  Our incoming capacity is in the hundreds of thousands of calls per day. With the addition of IVR and other technologies and channels such as chat, the capacity can be measured in the millions. Gatestone has the available skilled operator base and infrastructure to be able to handle large call volumes. Our American call centers have the capacity to accommodate hundreds of agents, and we have additional capacity in Canada, Mexico, Belize, and the Philippines. We have successfully on-boarded mid to large inbound and outbound contact and call center services for a wide range of clients over the last few years. Each of these programs were individually staffed with several dozen to hundreds of agents, with the two largest programs sustaining more than 600 agents each. These programs can confirm reasonableness of our ability and operational capacity to manage inbound calls and perform outbound calls, both similar in size and larger than the State of Nebraska's program.</p> <p>Gatestone's standard practice is to overstaff our workforce to account for any unexpected absence such as illness, vacation, or emergency circumstance, as well as to provide for a short-notice ramp-up as any assignment under this contract would necessarily be. Planned work schedules for all agents are 90% capacity in order to cover these situations and any potential call volume surges or seasonal increases. We are able to allocate any required FTE per any portfolio requirements within 24 hours' notice and complete client-specific training of reallocated staff for active operations within 72 hours' notice. We maintain a pool of cross-trained agents who are available for rapid allocation to any portfolio that requires additional staffing.</p>
12.	<p><b>Describe your capacity of in-house trainers and approach to on-boarding new call center staff to the project.</b></p> <p>Bidder's Response:  Gatestone's on-boarding and training approach and process is a combined function of our Human Resource and Training and Development Departments.</p> <p><b>Overview of our Human Resources Department</b>  Gatestone continually demonstrates its Human Resources experience in implementing successful BPO and call center projects and has documented its achievements, as well as lessons learned, from each onboarding experience it has completed over almost 100 years in operation.</p> <p>The company's project onboarding process is a function of the Human Resource (HR) Department and is managed by the Director of Human Resources with assistance from the recruiting and resourcing managers, human resource supervisors, employee engagement specialists, training and development managers, training officers and administrative support staff. These resources are all in-house.</p> <p><b>Onboarding Starts with Identifying the Right Candidate!</b>  Gatestone believes that in order to maintain a high-quality customer experience, it first starts with hiring the right talent. As such, Gatestone continues to invest in and refine our proprietary Gatestone Index (GI) behavioral assessment survey, which profiles individual characteristics and strengths matched to a job profile. This survey is administered on every potential candidate and employee at Gatestone and provides analytical information on their potential to succeed within a specific role. Additional details on the GI survey are provided in our Recruitment, Qualification and Hiring Process below.</p> <p><b>Recruitment, Qualification and Hiring Process</b>  Gatestone employs proven methods to efficiently recruit new candidates utilizing multi-channels such as; Internal referrals (Gatestone's referral program which is incentive based), websites, local job fairs, employment websites, community newspapers and language-specific websites, to name a few. Our recruitment, qualification, hiring and onboarding process is the same for all employees and follows the steps below;</p> <p><b>1. Job Analysis and Recruitment:</b> Once a job description and profile has been developed, Gatestone will publish the job opportunity to multiple market sourcing channels such as GatestoneTEQ intranet</p>

which promotes internal transfers, promotions or refer-a-friend cash incentive-based program, online career and job staffing websites, job fairs and other external posting forums such as colleges and universities.

**2. Pre-Screening and Testing:** Once a potential candidate has been identified, our Human Resources team performs a comprehensive review of the application. An initial telephone interview is conducted to assess communication skills, clarify and confirm BPO/call center experience, determine schedule availability, and provide an overview of the position and company and job expectations.

**3. GI Assessment:** Once a candidate has successfully passed Step 2, we administer the completion of a GI behavioral assessment survey, which profiles individual characteristics and strengths matched to a job profile. This survey identified candidates with the potential to succeed in the role they are applying for. Candidates GI results are analyzed by our in-house certified GI Analysts and compared to the profiles of top performers to mirror the attributes required to succeed as an agent. This tool has proven to reduce the time required to evaluate job compatibility and decrease likelihood of turn-over in both early-stages of employment and on an ongoing basis.

Through proprietary algorithms, the GI converts answers from a simple self-evaluation questionnaire into a skills and behavioral profile. By comparing resulting ratings within four elements, we are given a clear picture of the suitability for the job position.

### Overview of the Training and Development Department

All training and development for this initiative will be managed by our Training Manager, **Tracy Burks**. Tracy is supported by a large team of in-house Training Specialists who work together to develop and administer Gatestone's BPO/call center training and development programs, training related to internal and client policies and procedures and any program SOW and SLA requirements.

Tracy has been directly involved in developing and providing BPO/Call Center training to our employees since 2006 through our proprietary GatestoneTEQ (Training, Education, Quality) Learning Management System (LMS) platform. She is actively involved in a number of industry organizations in order to remain current and knowledgeable on regulations and best practices in BPO/call center operations and training techniques and holds Six Sigma Lean Professional, Corporate Trainer Certified, and Change Management Specialist certifications.

Gatestone's training approach includes classroom or virtual training, followed by on-the-job training and knowledge transfer across different roles. We utilize a number of training resources, including, simulations, AI training tools and our proprietary GatestoneTEQ, among other.

We understand and confirm our acceptance of the State's training as follows;

- The State-required training is approximately 16 hours.
- Additional in-house training by Gatestone is approximately 4-6 hours.

#### **Describe your staff retention policies and the average employee length of service.**

Bidder's Response:

Gatestone's approach to staffing retention includes several initiatives designed to improve productivity, retain talent and reduce turnover. In addition to specific initiatives and programs, Gatestone's firm policy of promoting from within gives employees the knowledge that they have a clear career path with the firm. Every senior operational executive, from the Chairman down, started as an agent. These retention initiatives include:

13.

- Full-time Employee Engagement Specialists responsible for a variety of internal communication projects, motivational campaigns, incentives and corporate savings endeavors across the company
- Incentives to boost employee morale, community building corporate charitable endeavours
- Gatestone Recognizes employee recognition and gift reward gamification platform
- Wellness initiatives, Staff Scholarships
- Sick leave bonus
- Absence control programs



Employee engagement is important to Gatestone. Our full-time dedicated Employee Engagement Specialists are responsible for a variety of internal communication projects, motivational campaigns, incentives and corporate savings endeavors across the company. They engage and inspire our staff to build more highly-effective working relationships across the company and promotes a positive working environment for all employees. These dedicated positions ensure employee satisfaction is at the highest level, thus reducing staff turnover and bottom line costs for our clients.

Gatestone’s approach to reducing attrition and managing absence is designed to improve productivity. This involves programs such as the following

- Incentives to boost employee morale: Gatestone has implemented numerous initiatives and incentives to reinforce our organization’s culture, support company goals and values, and boost morale, as follows:
- Over the course of the pandemic and at present, our leaders have engaged all employees in a work from home environment, to ensure their general well-being. We have implemented engagement strategies specifically targeted to our work from home employees to communicate Corporate and Leadership initiatives and we have also invested in additional engagement forums such as Social Media and town halls.
- We offer an employee recognition and gift reward gamification platform called Gatestone Recognizes. This platform allows the company to send gifts acknowledging milestones and performance.
- Tiered bonus programs and structures that reward a well-rounded agent’s performance and their contributions to each client’s program success. Some of the measurable KPIs considered for reward are productivity, quality, accuracy of work performed, collection statistics, etc.
- We provide a well-established formal employee management training program and a company philosophy of promoting high achievers. Clear and transparent succession planning is a priority. Several of our management team and leaders started in junior roles at Gatestone and have been promoted up the ladder through our leadership and development programs such as **Gatestone’s Got G.A.M.E.**, a program created to offer continuous development and leadership opportunities for resources identified as a good fit for succession.
- Access to Gatestone’s Employee Scholarship Program, specifically for employees to provide monetary support in direct advancement of a trade or industry by targeting certain fields of study.
- We engage new hires ahead of their start dates, with zoom info-sessions and regular emails about what to expect, so that they know Gatestone (as management and as a company) ahead of time.
- All senior executives of the company maintain an open-door policy, with engagement at all levels of the organization.
- All employees are well paid and have the opportunity to supplement their pay through performance incentives.
- On some programs we offer preferential scheduling with the opportunity to select the time slot of the work shift.
- Regular 30-minute Lunch and Learn training sessions and presentations to collaborate, learn, and drive personal, team, and business development.

Gatestone’s retention strategy includes implementing several initiatives and incentives with the goal of reinforcing our organization’s culture, supporting company goals and values and recognizing the many employees who go above and beyond. Since implementing these strategies, we have seen a significant increase in retention, year over year with **Agent average tenure trending around 6 years, which is considerably above industry standard.**

**Describe your ability to meet the reporting requirements set forth in Section V.C.2. including ad hoc reporting capabilities.**

14.

Bidder’s Response:

Gatestone confirms our ability to meet all reporting requirements as set forth in Section V.C.2 and will also provide any ad hoc reporting the State requires. We also understand that the Salesforce system is able to provide reporting on cases and that Gatestone will have the ability to create reports and dashboards regarding cases.

Our reporting deliverables for the State will include

1. Gatestone will submit a daily report via email or file sharing to the DHHS Contract Manager no later than 2:00 PM (Central Time) with the number of offered and handled calls, average speed of answer, and average handled time by queue for the previous day. The daily report will include

- completed items such as change requests, applications, statuses, and denials and also all outreach activities, as well as the quantity of other assigned calls or tasks for other work types.
2. Gatestone will submit to the DHHS Contract Manager by 12:00 noon on Tuesday of each week a weekly report that includes QA monitoring metrics, QA calibrations.
  3. Gatestone will provide ad hoc reports as requested by the State and understands that the due dates for ad hoc reports will be determined by both parties.

Gatestone provides access to a team of long-tenured in-house programmers and developers who offer a host of standard and customized ad-hoc reports. Our reporting offers full flexibility, and can be provided in any format of preference and timeline.

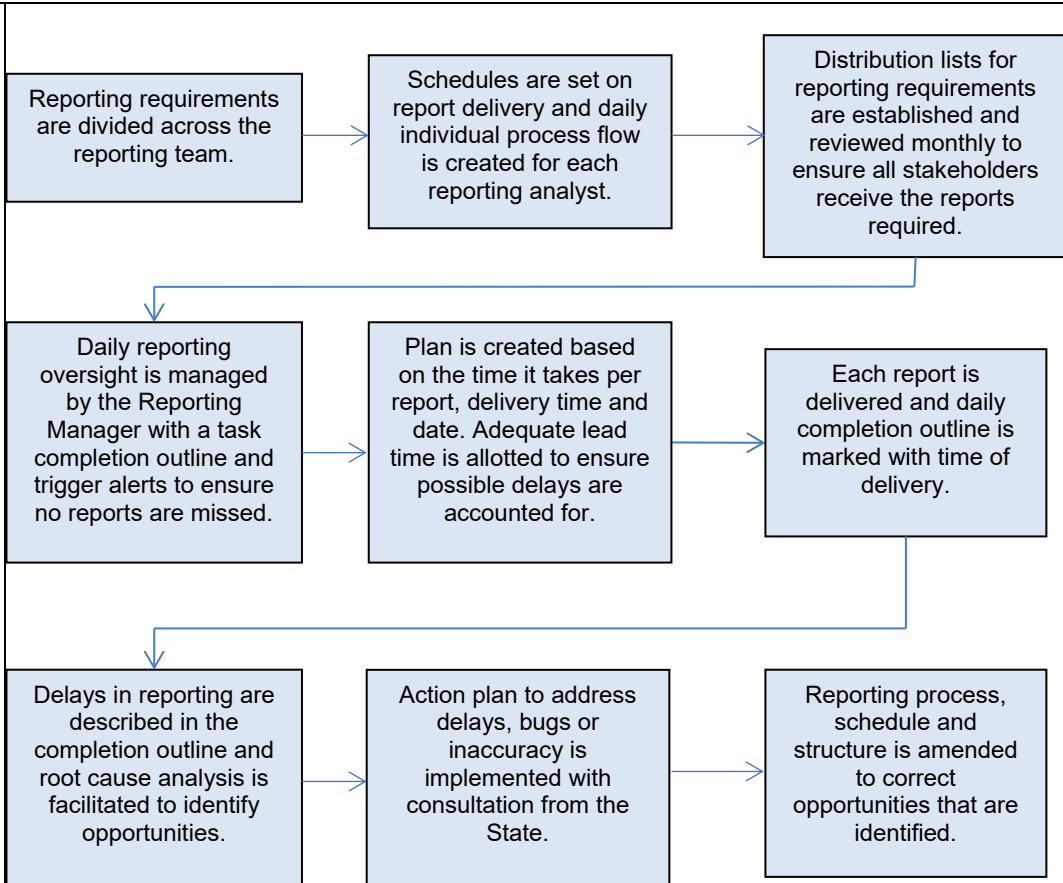
Gatestone is experienced in a host of BPO/call center reporting systems, both internally and also when utilizing the client's host system. Using these various reporting systems, we provide access to insight and eliminate a lot of the manual workload. Our reporting systems provide an intuitive reporting tool that displays a range of relevant BPO/call center metrics and KPIs that allow our Call Center Managers to monitor and optimize performance and identify emerging trends in a central location. The system also allows simplified analysis of information and significantly reduces data consumption time, allowing our reporting analysts to extract valuable real-time data easily. The online visualization tools have been proven to improve customer service intelligence through robust and easily customizable call center dashboards.

### **Reporting Management Structure**

The Reporting Manager oversees our Reporting Analysts who are fully trained and functional in all operational, staffing, volume and ad hoc reporting. Their day-to-day primary duties will be assigned in producing all the necessary reports for their designated service for the State. The reporting analysts will generate real-time performance dashboards to display daily, weekly and historical views of data required for the project.

### **Reporting Process**

Our reporting process flow chart is presented below.



## Reporting Analysis

Reporting analysis is facilitated by the Call Center Managers and Supervisors after reporting is created from the Reporting Analysts. The KPIs are analyzed for the following factors to determine opportunities:

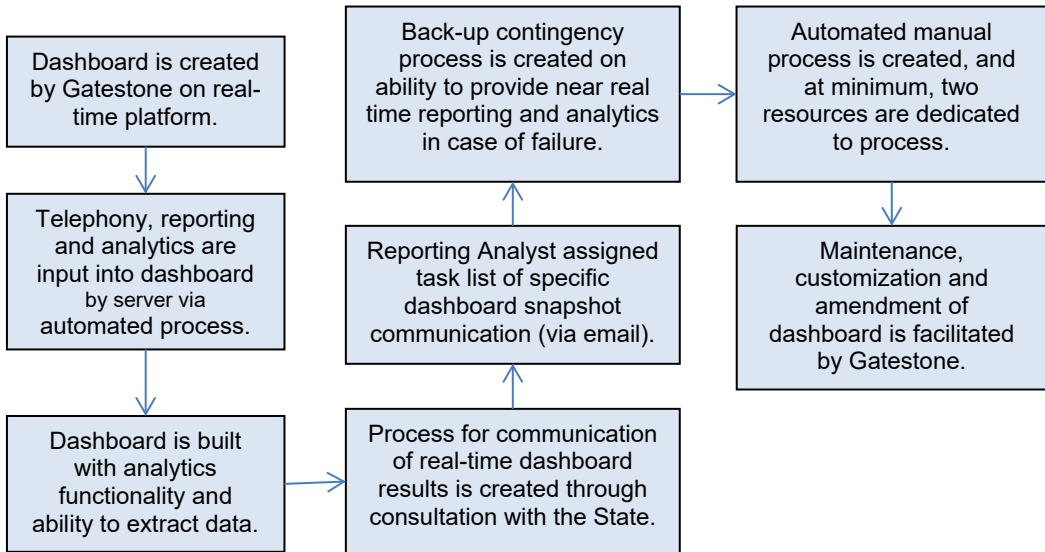
- Overall trend and performance in program
- Overall staffing and accuracy of forecasting
- Overall encounter quality and trends in program

Through determining the combination of which factor or combination of factors may be affecting the KPIs, the next steps involve a breakdown analysis of the agents working in that specific program.

- Individual performance and variance through scorecard analysis
- Individual schedule adherence
- Individual encounter quality

## Real Time Reporting on KPIs and SLAs

A flow chart detailing the process for real time reporting on KPIs and SLAs is presented below.



### Quality Scorecard to Monitor Performance

Gatestone utilizes a Quality Scorecard to score, review and analyze customer interaction recordings and agent performance. Team Leaders and Supervisors provide agents immediate evaluation, scoring and performance summaries using customized scorecard templates.

These scorecards are used to calibrate scoring among Quality Analysts, create targeted agent training plans and improve coaching sessions and will be customized with the State to address all the KPIs that are most important.

### Additional Standard Reports

Gatestone is able to provide additional standard reports around the State's ACCESSNebraska program which are included in our fees including:

- Dashboard reports
- Login and logout reports
- KPI metric report capturing the KPIs that are most important to the program
- IVR statistics report based on calls offered to switch, calls offered to queue, calls transferred and abandoned calls per language
- Interval report
- Line statistic reports
- KPI report and summary of bullet points where not meeting targets
- KPI report and management complaint handling / main contact reason ratio summary
- Forecast Report
- Target and goal report
- Root cause analysis report
- Quality analysis reports

15. **Describe how DHHS staff will access your Automated Call Distribution (ACD) software to view real-time wait times and available call capacity.**

Bidder's Response:  
 Our telephony platform, LiveVox, provides comprehensive and extensive reporting and real-time business intelligence capabilities to gain full insight into agent, team / campaign, and call center-level performance. All call data in the LiveVox platform can be reported on and viewed / exported as required and the State can be provided with logins alongside Gatestone in order to have direct access to data. Furthermore, we confirm that the solution will adjust and record the date and time of telephone calls as Nebraska local time.

LiveVox's business intelligence tool provides easy and instant access to insights across customer outcomes, staffing, quality, and compliance. Call center data visualizations let your team easily summarize data and key in on patterns, trends, and outliers.

This is key to success in distributed and hybrid office / work from home environments. The reporting and business intelligence (BI) tool has a user-friendly graphical user interface (GUI) to build reports across defined constraints and metadata, with a wide range of metrics and report columns available out of the box.

Reports can be viewed in the user interface, scheduled for regular delivery, and exported in standard formats for further downstream analysis.

Additionally, for real-time insights, LiveVox Wallboard is an independent web application that enables you to configure dashboards that display key performance indicators related to your call center volume (for inbound and outbound services) and agent or team productivity. Wallboard can display real-time metrics for the overall performance and progress of a call center (for example, average hold duration, average speed of answer, or call abandon rate). Wallboard can also highlight real-time problems that require the attention of a manager or supervisor (for example, when an agent has been in the same state for a long time, or when a service level agreement has been violated), through alerts.

A dashboard can be displayed on any screen such as a tablet, a desktop computer, or a widescreen office monitor, for private or public view, to enable you to monitor the activities related to your call center in real time. In general, a dashboard that appears on a large screen is called a wallboard. The Call Detail Report (CDR) provides information on all calls placed within defined parameters (e.g., date, campaign / queue, inbound phone number, etc.). Sample report screenshots are included below.

### Call Monitoring Report

The screenshot shows the 'Call Monitoring Report' configuration page. It features a blue header with the title and a search icon. Below the header, there are several filter sections. The 'Dates (MM/DD/YYYY)' section has 'From' and 'To' fields set to '09/01/2021'. The 'Call Center' and 'Agent' sections each have a 'Select One' dropdown menu. The 'Campaign' section has a 'Select One' dropdown. The 'Phone Dialed' section has a text input field. The 'Result' section has a 'Select Multiple Results' link. The 'Monitoring Event' section has a 'Select One' dropdown. The 'User' section has a 'Select One' dropdown. The 'Service' section has a 'Select One' dropdown. The 'Agent Team' section has a 'Select One' dropdown. The 'Campaign Pattern' section has a text input field. The 'Contact' section has a text input field. The 'Transfer Connect Duration' section has a 'Between' range selector with two text input fields. The 'Service Type' section has a 'Select One' dropdown. At the bottom right, there is a mouse cursor pointing at the interface.

### Configuration report

The screenshot shows the 'Customize Columns' dialog box for the Configuration report. The dialog has a blue header with the title. Below the header, there is a 'Customize Report Grid' section. This section contains a list of fields with checkboxes and a 'Select All' button. The fields are: Field (checked), Monitoring User (checked), Agent (checked), Agent Team (checked), Monitor Type (checked), Date (checked), Monitor Start Time (checked), Monitor End Time (checked), Total Duration (checked), and Call Center (checked). To the right of the list are two arrow buttons (up and down) for reordering. At the bottom of the dialog are 'Ok' and 'Cancel' buttons. In the background, a portion of the report grid is visible, showing columns for 'Center', 'Service Name', 'Campaign', and 'Acco'. A gear icon is visible in the bottom right corner of the report grid area.

### Agent Activity Report

Service	Customer Care ( 89950 )
Agent	NIRMALA agent.Delta
06/23/2021	
	10:13:50 10:16:55 00:03:04 00:00:00 00:00:00 00:02:27 00:00:37 0 0.00% 0 0.00 0 0 0 0 0.00 0.00%
	10:17:06 10:47:41 00:30:36 00:00:00 00:00:00 00:01:02 00:29:34 0 0.00% 0 0.00 0 0 0 0 0.00 0.00%
Day Totals	00:33:40 00:33:40 00:00:00 00:00:00 00:03:29 00:30:11 0 0.00% 0 0.00 0 0 0 0 0.00 0.00%
Agent Totals	00:33:40 00:33:40 00:00:00 00:00:00 00:03:29 00:30:11 0 0.00% 0 0.00 0 0 0 0 0.00 0.00%
Agent	SUSHEEL Susheel.Kums
06/29/2021	
	05:30:59 05:33:58 00:03:00 00:00:00 00:00:00 00:00:00 00:03:00 0 0.00% 0 0.00 0 0 0 0 0.00 0.00%
Day Totals	00:03:00 00:03:00 00:00:00 00:00:00 00:00:00 00:03:00 0 0.00% 0 0.00 0 0 0 0 0.00 0.00%
Agent Totals	00:03:00 00:03:00 00:00:00 00:00:00 00:00:00 00:03:00 0 0.00% 0 0.00 0 0 0 0 0.00 0.00%
Service Totals	00:36:40 00:36:40 00:00:00 00:00:00 00:03:29 00:33:11 0 0.00% 0 0.00 0 0 0 0 0.00 0.00%
Service	Manual - Agent ( 89737 )
Agent	NIRMALA agent.Delta
06/15/2021	
	02:25:06 23:01:09 20:36:03 00:00:00 00:00:00 01:30:15 19:05:48 0 0.00% 0 0.00 0 0 0 0 0.00 0.00%
	23:01:15 23:02:09 00:00:00 00:00:00 00:00:00 00:00:00 00:00:00 0 0.00% 0 0.00 0 0 0 0 0.00 0.00%
Day Totals	20:36:03 20:36:03 00:00:00 00:00:00 01:30:15 19:05:48 0 0.00% 0 0.00 0 0 0 0 0.00 0.00%
06/15/2021	
	01:10:00 01:10:00 00:00:00 00:00:00 00:00:00 00:00:00 00:00:00 0 0.00% 0 0.00 0 0 0 0 0.00 0.00%

### Agent Team Summary Report

#### Agent Team Summary Report

Dates (MM/DD/YYYY) From  To

Call Center  Service

Agent Team  Service Type

Show PTP Amount  Show Termination Codes

Show Detailed

#### Results

Successful Op T...	In Call (Min)	In Call (%)	Ready (Min)	Ready (%)	Wrapup (Min)	Wrapup (%)	Not Ready (Min)	Not Ready (%)	RPC : Payment/...	Non-Contacts	Total RPCs
1	0.40	0.25%	28.02	17.34%	1.28	0.79%	131.90	81.62%	0	0	0
1	0.40	0.25%	28.02	17.34%	1.28	0.79%	131.90	81.62%	0	0	0

### Call Recording Report

#### Call Recording Report

Dates (MM/DD/YYYY) From  To

Call Center  Service

Campaign  Campaign Pattern

Phone Dialed

Agent  Result

Sort By  Transfer Connect Duration Between  and


Service Type  Filename Search

#### Results

Service	Name	Contact	Phone	Agent	Session	Date	Start	End	Recordin...	Campaign	Result	Multimedia
IB Skill		123	6503517493	LV_QA	U2C67CT5DF5CC1	Sun Dec 20 2021	9:16:40 AM	9:16:50 AM	10	1000555_CALLBAC	AGENT - B	0
IB Skill		123	6503517493	LV_QA	U2C099T5DF6AD3	Sun Dec 20 2021	10:16:41 AM	10:16:44 AM	2	1000555_CALLBAC	AGENT - B	0

Our system produces more than 100 pre-formatted reports that can be run in real-time. Therefore, we can accommodate virtually any information request from the State immediately. Our reporting varies from client to client and we customize all reports and meeting agendas to comport with our clients' needs. We are able to provide any information in these meetings that the State may wish to receive - it is entirely up to you. Gatestone will establish a reporting and analytics system to monitor program performance. Gatestone is experienced in a host of reporting systems, both internally and also when utilizing a client's host system. Using these various reporting systems, we provide access to insight and eliminate a lot of the manual workload. Our call center reporting system platform provide an intuitive reporting tool that

	<p>displays a range of relevant metrics and KPIs that allow our leadership to monitor and optimize performance and identify emerging trends in a central location. Further, Gatestone has a dedicated reporting department, staffed with teams of reporting analysts and programmers to ensure robust client reporting.</p> <p>Our standard dashboard reports will be provided in a timeframe as required by ACCESSNebraska (daily, weekly, monthly), and are included in our fee. Reports include (but are not limited to):</p> <ul style="list-style-type: none"> <li>■ Agent attrition report</li> <li>■ Capacity and resource summary report</li> <li>■ Login and logout report</li> <li>■ KPI performance metric report capturing the KPIs that are most important to the program</li> <li>■ IVR statistics report based on calls offered to switch, calls offered to queue, calls transferred to agent and abandoned calls per language, top and bottom performer</li> <li>■ Interval report</li> <li>■ Line statistic report</li> <li>■ KPI report and summary of bullet points where not meeting targets</li> <li>■ KPI report and management complaint handling / main contact reason ratio summary</li> <li>■ Forecast report</li> <li>■ Target and goal/sales report</li> <li>■ Cost of poor performance report</li> <li>■ Root cause analysis report</li> <li>■ Quality and compliance report</li> </ul> <p>Additional reports that are available to the State include any additional ad hoc (customized) reports, quality analysis reports, and a benchmark performance report.</p>
16.	<p><b>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.</b></p> <p>Bidder's Response:  Gatestone does not do any software development and uses off the shelf software. We ensure our 3rd parties have a proper SDLC and software escrow. Gatestone has worked with and has the ability to provide CRM's such as: Salesforce, ZenDesk, Oracle, MS Dynamics, ServiceNow, SAP, Sugar CRM, any many more. Our inhouse CRM is Spiro, which has been customized for Gatestone. Some of the capabilities our CRM enables include:</p> <ul style="list-style-type: none"> <li>■ Intelligent record creation - The Spiro Assistant automatically creates contacts, companies, and opportunities from conversations over email</li> <li>■ Enriched company + contact details - Company records are supplemented with data like LinkedIn profiles, phone numbers, and addresses</li> <li>■ Consolidated customer touchpoints - Spiro captures every interaction with a prospect or customer, including emails, calls and texts, notes, and meetings</li> <li>■ Capture details in the moment - Automated call logging ensures that crucial details and next steps are easily captured – in the moment</li> <li>■ Call transcriptions - Whether it's for coaching or reviewing details, dive deep into conversations with Spiro's call transcriptions</li> <li>■ Simplified pipeline management - Spiro's pipeline views allow for efficient contact management</li> <li>■ Improved account relationships - Spiro integrates with your business systems and then proactively recommends actions to improve customer engagement</li> </ul>

	<b>No.</b>	<b>Approved by</b>	<b>Effective as of</b>	<b>Document Title</b>	<b>Owner</b>	<b>Classification</b>
	7.9	Robert Coats	Aug 17 <sup>th</sup> 2021	Gatestone Security Policy	Information Security Department	Confidential – only to be used by Company


## Gatestone Physical Security

Classification: Confidential

### Summary of Changes

Date	Issue	Description	Authorized by
April 19 <sup>th</sup> 2011	6	Annual review of security document.	Robert Coats
March 1, 2012	6.1	Rebranding	Robert Coats
May 22 <sup>nd</sup> 2012	7	Review Document. Removed Gordon Baker and changed sign in required for computer room.	Robert Coats
Feb 10 <sup>th</sup> 2014	7.1	Minor changes to CCTV	Robert Coats
Feb 17 <sup>th</sup> 2014	7.2	Approved by Management Signature area	Robert Coats
June 21 <sup>st</sup> 2015	7.3	Cipher/Combination lock addition	Robert Coats
June 29 <sup>th</sup> 2016	7.3	Annual review no changes	Robert Coats
Sept 30 <sup>th</sup> 2016	7.4	Added retention time	Robert Coats
Jan 25 <sup>th</sup> 2018	7.5	Added requirement to review badge access bi-annually	Robert Coats
March 3 <sup>rd</sup> 2018	7.5 6	Changed camera CCTV portion to 90 days due to changes in client requirements	Robert Coats
May 5 <sup>th</sup> 2018	7.6	Changed fire drill to annually to align with building management. Manual key management changed to executive assistants only. Building does not have a copy.	Robert Coats
July 19 <sup>th</sup> 2018	7.7	Changed retention for Capital one to 12 months from 6 months	Robert Coats
Aug 1 <sup>st</sup> 2019	7.9	Added Edwin to escalation call list for Perigrin	Robert Coats
Sept 11 <sup>th</sup> 2019	7.9	Minor change in schedule for shredding and hard drive destruction.	Robert Coats



	<b>No.</b>	<b>Approved by</b>	<b>Effective as of</b>	<b>Document Title</b>	<b>Owner</b>	<b>Classification</b>
	7.9	Robert Coats	Aug 17 <sup>th</sup> 2021	Gatestone Security Policy	Information Security Department	Confidential – only to be used by Company


<b>Date</b>	<b>Issue</b>	<b>Description</b>	<b>Authorized by</b>

Last reviewed: Aug 17<sup>th</sup> 2021  
Robert Coats

## REVIEW PROCESS: Annual review.

<b>Date</b>	<b>Issue</b>	<b>Description</b>	<b>Authorized by</b>
Aug 17 <sup>th</sup> 2021	7.9	Review of document...Formatting changes and few typo fixes..No other changes	Robert Coats
Aug 8 <sup>th</sup> 2020	7.5	Review of document.. No changes	Amir Butt
Aug 1 <sup>st</sup> 2019	7.5	Review of document.. some changes to escalation call isit.	Robert Coats
Jan 25 <sup>th</sup> 2018	7.4	Annual review	Robert Coats
June 23 <sup>rd</sup> 2017	7.3	Review of Document.. No changes	Robert Coats
June 29 <sup>th</sup> 2016	7.2	Review of document conducted	Robert Coats
Jun 2 <sup>nd</sup> 2015	7.1	Changed locations to 180 Duncan Mill and added fire evacuation dates	Robert Coats
Feb 10 <sup>th</sup> 2014	7	Add requirement for CCTV to be in secure area.	Robert Coats
June 3 <sup>rd</sup> 2013	6	Review of document. No changes	Robert Coats
May 22 <sup>nd</sup> 2012	5	Review Document. Removed Gordon Baker and changed sign in required for computer room.	Robert Coats

Last reviewed: Aug 17<sup>th</sup> 2021

	No.	Approved by	Effective as of	Document Title	Owner	Classification
	7.9	Robert Coats	Aug 17 <sup>th</sup> 2021	Gatestone Security Policy	Information Security Department	Confidential – only to be used by Company

## Roles and Responsibilities

The responsibility for physical and environmental security will vary among the Offices depending upon organization structure and facility arrangements (i.e., owned, leased or shared). These responsibilities may cross divisions/offices authorities and be assigned through written agreement or contract. Key roles that affect the implementation of this policy are:

**Information Security Officer-** shall ensure the policy and procedures are written, disseminated and adhered to. A yearly review of the physical security will be done to ensure compliance.

**Facility Managers** – All Offices shall have facility management. This function may be outsourced (e.g., with leased buildings) or there may be a Gatestone representative assigned to one (1) or more buildings.

**Visitor Control Personnel** – All buildings shall have visitor control procedures.

**Safety Officers** – Each facility shall have designated emergency evacuation personnel that will ensure that emergency evacuation routes are clearly posted, emergency response procedures documented, tested are distributed to all building personnel.


**Network and Computer Operations Management** - All network and computer operations managers/administrators shall be responsible for the physical security of the hardware and software assets assigned to them.

**Managers and Supervisors** – All Office Managers and Supervisors responsible for operations shall ensure that adequate physical security is provided to protect assets.

**Contracts Administration** – Contracts administration shall ensure that third party agreements provide the level of security defined in policies. Gatestone contracts and interagency agreements shall contain the necessary physical security provisions to protect sensitive and critical information in the work stream.

**Employees/Contractors/Volunteers** – All Gatestone employees/contractors/volunteers have an obligation to protect Gatestone physical assets.

Policy implementation shall be based upon the use of management-approved security standards and in coordination with the Information security officer senior management. The following paragraphs specify the physical and environmental policy requirements in order to address Information Technology Services (ITS) security.

	No.	Approved by	Effective as of	Document Title	Owner	Classification
	7.9	Robert Coats	Aug 17 <sup>th</sup> 2021	Gatestone Security Policy	Information Security Department	Confidential – only to be used by Company

1. Facility Security (Building) shall be provided at all Offices. This will include facility management. Facilities may utilize guards and/or surveillance monitoring when necessary. Offices shall ensure that its facilities have implemented adequate physical and environmental security necessary to protect its information resources within budgetary resources. Information Security officer and senior management are to prepare and maintain a facility security plan. This document shall include building records, vendor contact lists, physical security contract information, and key control procedures. This information shall be included as appropriate in the division/office business continuity plan.


Controls which will be monitor include loss of power, UPS failure, fire, high temperature, water, humidity, door forcing and motion detection

2. Physical Access Control (Internal/External); Gatestone offices are responsible for providing adequate physical security in the workplace. Gatestone shall implement physical access control procedures at designated points where personnel access needs to be limited. All entrances and exits will have security badge access systems which is monitored .The Gatestone workforce (employees/contractors/volunteers) shall receive badges and display them properly, so they are clearly visible, at all times within the office. Areas where information is stored, processed, server rooms, data rooms and payment processing areas will be restricted by a badge access system with only users who need this function. A list of all individuals with access to these controlled areas (Switch rooms and servers with client information) will be kept and reviewed once per year along with this document. Emergency keys to these areas will be held by the executive assistants in the secure executive area. Access is given on an emergency basis only and logged as to whom it was lent to and when it was returned. These keys are not able to be copied and are replaced when the building or office manager cease to be employed by Gatestone or is transferred to another department.

A UPS will be setup to protect the equipment sensitive to surges in power.

3. Visitor Control: Gatestone offices shall implement visitor control procedures that may include any or all of the following features:

- A. Visitor log maintained.
- B. Sign-in/sign-out procedures with time recorded for both datacenter and front desk.
- C. Temporary badge with tracking number properly displayed.
- D. Visitor escorted at all times in accordance to procedures developed in accordance with the visitor security policy.
- E. Name of the person visiting
- F. Signature of the visitor

 <b>GATESTONE</b>	<b>No.</b>	<b>Approved by</b>	<b>Effective as of</b>	<b>Document Title</b>	<b>Owner</b>	<b>Classification</b>
	7.9	Robert Coats	Aug 17 <sup>th</sup> 2021	Gatestone Security Policy	Information Security Department	Confidential – only to be used by Company

- G. Form of identification
- H. Date of access
- I. Purpose of visit

E. Visitor access logs are to be reviewed annually to ensure compliance with policy.

4. Closed-Circuit TV (CCTV) camera Surveillance Monitoring at the Gatestone Offices shall be performed at all entrances, exits and restricted areas, to ensure workforce safety and prevent property loss. Surveillance monitoring shall be limited to areas perceived as high risk unless otherwise required. CCTV data will be kept for 90 days in a secure environment.

- This will be verified working on a weekly basis by the physical security administrator . This will be recorded on a checklist .

5. Protecting the Technical Infrastructure Offices shall provide the level of physical and environmental protection of its technical infrastructure as specified by the information security officer (ISO) to minimize the risk of unauthorized access or environmental hazards. The ISO shall collaborate with the requesting of funding of and remediation of the physical and environmental factors as required.


6. Work Area Security The employee/contractor work area shall be properly secured to protect both sensitive and critical information and ensure privacy. Workstations shall be placed in a location that protects the confidentiality of data. Documents and media shall be stored in a secure manner.

7. Physical Inventory Control is to be maintained by the help desk, which is a formal inventory of assets (hardware, software and applications) for the Offices. Asset inventory shall be performed at regularly scheduled intervals or when a significant change has occurred or a year has passed.

8 Power Protection Offices shall provide power protection to support both personnel safety and ensure the availability of its information systems. All sensitive and critical information processing systems shall be protected by an uninterruptible power supply.

9. Physical Security of Telecommunications Resources; The telecommunications lines and equipment of Gatestone Offices shall be adequately protected to ensure both availability and the confidentiality of this resource. Sensitive information shall only be sent over secure lines. The ISO of Information Resource Management and the Office of Property and Construction shall ensure that adequate safeguards are in place.

10. The off-site storage facilities for Gatestone offices shall be afforded the same level of protection as the main processing site. Adequate physical security and environmental controls shall be implemented to protect the data.

	No.	Approved by	Effective as of	Document Title	Owner	Classification
	7.9	Robert Coats	Aug 17 <sup>th</sup> 2021	Gatestone Security Policy	Information Security Department	Confidential – only to be used by Company


11. Controls for Environmental Exposures in the Workplace Offices shall protect both personnel and assets by implementing controls that will protect the environment from environmental hazards. These controls include but are not limited to: Temperature and humidity controls, smoke detectors, floods and fire suppression systems. Temperature will be kept between 14 and 21 Celsius in the “Operations room” and humidity between 40 and 60 percent.

12. Mobile Computing Devices Security (Laptops, PDAs, etc) Laptop computers shall be issued only to authorize division/office personnel who shall be responsible for both the physical security and the information stored on the device. All laptops shall be inventoried with a property tag or barcode shall be password protected to limit access to its authorized user,. The ISO shall develop and maintain enterprise-wide standards and procedures for implementing laptop security. Any use of PDAs and other mobile computing devices must meet the required security standards and be approved by the ISO. The use of PDAs or smart phones, etc. to access and log personally identifiable information at Gatestone is restricted and access should be granted only under approved circumstances. Documentation of authorization shall be retained by the ISO. The user is responsible for seeking authorization from the ISO and notifying the supervisor of any changes in use of or type of equipment. The ISO, in consultation with office staff, shall develop and maintain enterprise-wide procedures for implementing PDA security. Any authorized use must also be in compliance with the Gatestone Acceptable Use Systems Policy. Wireless access to the network and its related equipment and components is not allowed presently

13. Property Control Any movement of information, software media, hardware or other physical assets shall be strictly controlled. Only authorized personnel shall be permitted to take Office property off the premises and they shall be responsible for protecting the property and controlling its use. Gatestone ISO shall develop and maintain enterprise-wide procedures for ITS property control, in consultation with office staff.

14. Removable Storage Devices. The use of removable storage devices or external devices (e.g.; USB Flash Drives) shall be restricted to authorized personnel in order to safeguard and protect confidential data and information technology assets. Authorization for the use of removable storage devices must be granted by the user’s supervisor in writing and specify the intended use of the device. Documentation must be maintained according to division/office procedures and minimally include: Identification of staff, identification of job functions requiring the use of a removable storage device, type of device utilized, knowledge of standards and policies, and signatures of authorized staff and supervisor signifying acceptance of conditions. The ISO shall be responsible for the development and revisions of policy and standards as technology advances.

15. Safety and Emergency Procedures; Gatestone offices shall regard personnel safety as a high priority and take the necessary steps to ensure a safe workplace. The ISO shall

	No.	Approved by	Effective as of	Document Title	Owner	Classification
	7.9	Robert Coats	Aug 17 <sup>th</sup> 2021	Gatestone Security Policy	Information Security Department	Confidential – only to be used by Company


develop, in collaboration with other responsible division/offices and the Safety Director, enterprise-wide emergency procedures for handling a variety of threats. Emergency evacuation procedures shall be written, maintained and tested on annual basis at each facility and reviewed annually to ensure its operational capabilities. Power to all equipment will have a breaker system capable of detecting a short and shutting down and or allowing for manual shutdown remotely.

17. Incident Management Incidents shall be managed and reported as required in the Gatestone Security Incident Management Policy.
18. Disposal of Sensitive Documents, Media and Equipment Gatestone sensitive documents, media and equipment must be disposed of in an approved manner that protects the confidentiality of the information printed or stored. Refer to the classification matrix for examination of the disposal methods.
  - A. Disposal of sensitive documents.
  - B. Destruction of computer equipment that may contain sensitive information
  - C. Sanitization (i.e., object reuse) of equipment that might be sold or transferred to other organizations.
  - D. Destruction of various types of media.

Hard drives for destruction are kept in a bin in a secure room and scheduled for destruction once a year.

19. Physical Site Inspections a physical security inspection shall be performed periodically by the ISO to ensure policy compliance. The inspection process, including but not limited to the schedules of guards, Cameras, badge access , locks, doors , fire alarms, air conditioning, water detection , motion detection, UPS, generator and any other physical security devices required. and results of the inspection shall be coordinated with property management and any construction firm tasked with remediation. The ISO shall notify the Gatestone senior management of the results of physical security inspections for the purpose of remediation of deficiencies.

Description of Facility:

	No.	Approved by	Effective as of	Document Title	Owner	Classification
	7.9	Robert Coats	Aug 17 <sup>th</sup> 2021	Gatestone Security Policy	Information Security Department	Confidential – only to be used by Company

180 DUNCAN Mill road has the following, 3rd floor contains Reception, Boardroom, Management offices, Accounting, Sales and Client Services, a reception area for people making payments, the Cash Office, Human Resources, legal offices and Information Technology. The 2<sup>nd</sup> and 3<sup>rd</sup> floors house receivable management Operations.

Access to Gatestone is through the front doors at Duncan Mill or through a laneway at the rear of the building. . Closed circuit cameras are in use. Access to the building floors is through a bank of elevators and two fire stairwells. After hours use of the elevators is restricted by security card.

The buildings are run by Avis and Yonge Property Management. Paragon Security is the company which provides security guards and Peregrine Security is the company which supplies and maintains the security system in the building.

Visitors to the building are required to sign in with front Desk Security on the 3<sup>rd</sup> floor. All access points are secured through a security card swipe set up. Each company has their own set of security cards. All cards are to be swiped each time you enter a door. No one is to ‘Piggy back’ behind another person entering another area.

Human Resources track all security cards and the access they have to correlate to the person using it. Employees are required to sign security forms upon hiring. Anyone who is caught breaching the security policies of the company is subject to immediate dismissal.


**Physical Security Elements**

Secure data areas where client information is stored will floor to wall ceilings to prevent entering of premises. Motion detection will also be placed in the data center connected to an alarm company 24 hours a day.

Photo Id must be worn by all employees at all times. If a photo ID or access swipe card is lost or stolen then this is to be reported to Human resources immediately who will deactivate it.

Gatestone maintains its own internal security card system. Collectors and most employees are restricted to the floor on which they work and the lunchroom. Approval at the executive level is required before access is given to other locations and is restricted to work duties. Computer room access is limited to systems operations group plus the Corporate Security Officer. Employees are to use their card to access the floor each and every time they enter. No one is to use another employees card not ‘piggy back’ behind someone else.

**Log Retention:**

	No.	Approved by	Effective as of	Document Title	Owner	Classification
	7.9	Robert Coats	Aug 17 <sup>th</sup> 2021	Gatestone Security Policy	Information Security Department	Confidential – only to be used by Company

1. Badge access logs to be kept for 12 months.
2. Visitor access logs are to be kept for 12 months.
3. Camera footage will be kept for 90 days.

**Badge reconciliation:**

Badge access of all users will be reviewed bi-annually to ensure

1. a single badge is assigned to a user
2. User access to restricted areas are correct
3. Ensure badges not assigned are disabled

Cipher of Combination locks:

Where the use of cipher locks if used the combination will be changes annually.

Video surveillance is available on all floors, hallways, reception, and computer room.

Firewall protection is provided by Firebox IDS appliance from Watchguard technologies and all gateways, servers and workstations are protected with Sophos Anti-virus protection that is updated daily. The exchange servers are protected with Sophos anti-virus software that is updated hourly.

All workstations are hardened and have all floppy and CD drives removed or disabled.


Locked shredding bins are located on the floors and secured monitored service is used for disposal. The shredding will be observed by a member or Gatestone to ensure compliance. The shredding will be complete using cross cut shredding. The paper will be stored in locked containers and emptied before they are full. Regardless of being full shedding service is scheduled for every two weeks.

All employees are required to sign the security policy acceptance form upon being hired, Security cameras record all activity at all access areas, a fireproof, key lock safe secures cash office information.

Access logs and videotapes/hard disks are retained for a period of Twelve months. They are protected inside the computer room, which requires the highest level of access and is restricted on an as needed basis to a very small number of people.

Security alarms are monitored by Peregrine protection home alarm security. Upon an alarm going off, a security guard is dispatched to the area where the security alarm has detected a problem. Edwin Saldanha, Nilda Mejias and Robert Coats will be notified then decide on further escalation.



	<b>No.</b>	<b>Approved by</b>	<b>Effective as of</b>	<b>Document Title</b>	<b>Owner</b>	<b>Classification</b>
	7.9	Robert Coats	Aug 17 <sup>th</sup> 2021	Gatestone Security Policy	Information Security Department	Confidential – only to be used by Company

All visitors and employee’s without access to Gatestone premises are required to sign in at reception and datacenter separately. They are required to wear a visitors badge and are accompanied by a Gatestone agent at all times.

All doors are to have an audible alarm sound if left open for longer then 60 seconds.

Evacuation Test Schedule tested biannually.

Next Test

Phoenix:	October	2012	Complete	April 2013
Phoenix	April	2013	Complete	April 2014
Phoenix	April	2014	Complete	April 2015
Duncan Mill	Oct	2015	Complete	October 2016
Duncan Mill	June	2016	Complete	May 2017
Duncan Mill	May	2017	Complete	April 2018
Duncan Mill	Feb	2018		

Addendum1:


NOTE: The Phoenix computer room has 2 entrances. The entrance without the badge access will have its door locked at all times with the purpose of keeping out all users who do not have an assigned badge.. This computer room will have motion detection with a 3<sup>rd</sup> party company monitoring that will detect any entrance to this room without triggering the badge system firs. Calling tree will include senior executives.

## Approvals:

Name: Robert A Coats  
Title: Information Security officer

Signature:

Name: Claude LaPointe

	<b>No.</b>	<b>Approved by</b>	<b>Effective as of</b>	<b>Document Title</b>	<b>Owner</b>	<b>Classification</b>
	7.9	Robert Coats	Aug 17 <sup>th</sup> 2021	Gatestone Security Policy	Information Security Department	Confidential – only to be used by Company

Title: Associate Vice President

Signature:

Name: Nilda Mejias

Title: Computer Operations Manager

Signature:



# Gatestone & Co. Security Policy

---

Confidential

**Robert Coats**

## Summary of Changes

Date	Issue	Description	Authorized by
Feb 4 <sup>th</sup> 2022	34.1	Change password policy to be 14 character s to programmatic accounts.	Robert Coats
Oct 13 <sup>th</sup> 2021	3.4	Added keeping investigation logs for 3 years instead of the current 13 month.	Robert Coats
April 28 <sup>th</sup> 2020	3.4	Review of document no changes	Robert Coats
April 15 <sup>th</sup> 2019	3.4	Added insider Threat policy	Robert Coats
July 20 <sup>th</sup> 2018	3.3	Removed Kim Prado and added Claude LaPointe to the document	Robert Coats
July 16 th 2018	3.2	Added the requirement to change default ID's on equipment as well.	Robert Coats
June 14 <sup>th</sup> 2018	3.1	Addition of the PIPA regulation required by Alberta and BC regulations. Change to encryption requirement from Sha 1 to Sha256	Robert Coats
May 19 <sup>th</sup> 2017	3.0	Minor encryption changes required for alignment with our clients. Deprecated TLS .	Robert Coats
Dec 19 <sup>th</sup> 2016	2.9	Added international law requirement for encryption	Robert Coats
Nov 17 <sup>th</sup> 2016	2.8	Change verbiage in encryption policy to include ATT requirement to be encrypted during transport and the files itself. Also change encryption at rest to be immediately instead of 24 hours.	Robert Coats
Aug 30 <sup>th</sup> 2016	2.7	Added the requirement for a DMZ and DDOS protection.	Robert Coats
June 29 <sup>th</sup> 2016	2.6	Added destruction standard for Disk drives in destruction matrix. Require all Disks including As400 to be destroyed by physical destruction. Page 26	Robert Coats
April 25 <sup>th</sup> 2016	2.5	Added a small change to project management to separate the duties of the requestor, approver and implementer.	Robert Coats

Last reviewed Jan 2022  
Robert Coats

## REVIEW PROCESS: Annual review.

Date	Issue	Description	Authorized by
Jan 2022	3.41	Changes to password policy to include programmatic account use 14 character	Robert Coat
May 2021	3.4	No changes after review	Robert Coats
April 28 <sup>th</sup> 2020	3.4	No changes after review	Robert Coats
April 2019	3.4	Review and addition of insider threat policy	Robert Coats
June 12 <sup>th</sup> 2018	3.1	Annual review.. remove d reference to specific locations and added PIPA act to required regulatory requirements	Robert Coats
Feb 3 <sup>rd</sup> 2017	2.9	Annual Review No changes to document needed.	Robert Coats
Jan 14 <sup>th</sup> 2016	2.4	Annual Review	Robert Coats

Last reviewed: Jan 2022

**Index**

Commented [RC1]:  
Commented [RC2]:

**INDEX ..... 3**  
**EXECUTIVE SUMMARY ..... 7**  
**INFORMATION SECURITY TEAM MEMBERS ..... 7**  
**POLICY CREATION GUIDELINE ..... 7**  
**ACCEPTABLE USE POLICY ..... 7**  
    MONITORING OF EMPLOYEES..... 8  
    UNACCEPTABLE USE..... 8  
**EXCEPTION TO POLICY ..... 9**  
**VISITORS ACCESS POLICY .....10**  
**ACCESS CONTROL POLICY.....11**  
    SUMMARY ..... 11  
    NEW EMPLOYEES/CONTRACTORS: ..... 12  
    TERMINATED OR RESIGNING EMPLOYEES/CONTRACTORS: ..... 12  
    OTHER USERS' MAINTENANCE (PROMOTIONS, TRANSFERS, CONTRACTORS ETC.) 13  
    BUILDING EMPLOYEES..... 13  
**HIRING POLICY .....13**  
    ACCESS AUDITING AND ENTITLEMENT REVIEW ..... 14  
    ENFORCEMENT ..... 14  
**ANTI-VIRUS POLICY .....15**  
**AUDIT POLICY .....15**  
**SECURITY ASSESSMENT AND CERTIFICATION .....16**  
    REQUIREMENTS OF ALL CHANGES..... 17  
    REQUIREMENT OF MANAGEMENT: ..... 17  
**ASSET CONTROL .....17**  
**INFORMATION SENSITIVITY POLICY .....18**  
    SECURITY AND PROPRIETARY INFORMATION ..... 18  
    CLASSIFICATION OF INFORMATION ..... 18  
**DATA AND MEDIA CLASSIFICATION AND PROTECTION MATRIX ..19**  
    NON SENSITIVE ..... 19  
    SENSITIVE ..... 19  
    PUBLIC           NON PUBLIC ..... 19  
    CRITICAL ..... 19  
    RESTRICTED ..... 19  
    PENALTY FOR DELIBERATE OR INADVERTENT DISCLOSURE: ..... 23  
    LABELING POLICY..... 23  
**AVAILABILITY CONTROLS .....24**  
    PRESENT CONTROLS..... 24  
**PHOTOGRAPHIC AND RECORDING DEVICE POLICY .....24**  
    PURPOSE: ..... 24  
**RISK ASSESSMENT POLICY .....25**  
    MISSION STATEMENT ..... 25  
    EXPLANATORY NOTES..... 25  
    RISK ASSESSMENT REQUIREMENTS ..... 25  
**ENCRYPTION POLICY .....26**  
    ENCRYPTION MISSION STATEMENT..... 26  
    EXPLANATORY NOTES..... 26  
    ENCRYPTION: RESPONSIBLE PARTIES..... 26  
    ENCRYPTION: REQUIREMENTS ..... 26

ENCRYPTION/MASKING: REQUIREMENTS CREDIT CARD NUMBERS:	27
<b>PASSWORD AUTHENTICATION AND IDENTIFICATION PROTECTION POLICY</b>	<b>28</b>
SERVICE ID PASSWORDS	29
PROCESS REQUIREMENTS	29
ROLES AND RESPONSIBILITIES	30
<b>ACCOUNT REVIEW POLICY</b>	<b>30</b>
<b>ROUTER SECURITY POLICY</b>	<b>30</b>
<b>NETWORK SECURITY POLICY</b>	<b>32</b>
CABLE INSTALLATION AND MANAGEMENT PROCEDURES	32
<b>SERVER AND WORKSTATION SECURITY AND MAINTENANCE POLICY</b>	<b>33</b>
OWNERSHIP AND RESPONSIBILITIES	33
GENERAL CONFIGURATION GUIDELINES	34
MONITORING	35
COMPLIANCE	35
TECHNICAL COMPLIANCE	35
HARDENING OF SERVERS:	38
<b>PATCH MANAGEMENT AND END OF LIFE SOFTWARE CONTROL:</b>	<b>39</b>
PATCH MANAGEMENT FOR NON-WINDOWS SYSTEMS	39
<b>REMOTE USER ACCESS CONTROL POLICY</b>	<b>39</b>
REMOTE ACCESS - TWO-FACTOR AUTHENTICATION	40
REMOTE ACCESS – REQUESTS	40
REMOTE ACCESS – CONFIGURATION AND CONTROL	40
REMOTE ACCESS – MANAGEMENT AND MONITORING	41
REMOTE ACCESS CHECKLIST	41
REMOTE ACCESS – SECURITY OFFICER RESPONSIBILITIES	42
REMOTE ACCESS – USER RESPONSIBILITIES	42
<b>ACCESS AND SYSTEM MONITORING POLICY</b>	<b>42</b>
PCI INFORMATION	43
CLIENT FILE ACCESS INFORMATION	43
ANTIVIRUS ALERTS	43
INTERNET TRAFFIC:	43
MAIL:	44
LOGON INFORMATION:	44
<b>FIREWALL BUILD POLICY</b>	<b>45</b>
PRINCIPLES:	45
OPERATION:	45
CONFIGURATION:	45
FIREWALL DETAILED CONFIGURATION:	45
FIREWALL CHANGE CONTROL:	46
CONTINGENCY PLANNING:	50
SECURE BACK-UP:	50
POSTING UPDATES:	50
MONITORING VULNERABILITIES:	50
AUDIT AND COMPLIANCE	50
<b>IDS (INTRUSION DETECTION):</b>	<b>51</b>
LOG STORAGE:	51
MONITORING:	51
BACK UP LOGS:	51
<b>PROJECT MANAGEMENT AND CHANGE MANAGEMENT CONTROLS</b>	<b>52</b>
PROJECT DEFINITION	52

PROJECTS CLASSIFICATION .....	52
PROJECT PLANNING .....	53
RISK ASSESSMENT AND SECURITY PLAN .....	53
TESTING AND QA .....	53
TESTING LEVELS .....	54
TEST CASES .....	54
SECURITY TESTING .....	54
TEST DATA .....	55
BACK OUT PLAN .....	55
POST IMPLEMENTATION TESTING .....	55
CODE REVIEW .....	55
PROJECTS APPROVALS AND IMPLEMENTATION: .....	55
PROJECTS DATABASE .....	56
<b>DEVELOPMENT AND PROGRAMMING .....</b>	<b>56</b>
TABLES .....	56
MODULES .....	57
INTELEC PROGRAMS .....	57
LIBRARY REFERENCES .....	57
NAMING CONVENTION .....	57
VALIDATIONS .....	58
PROGRAMMING LANGUAGES .....	58
GENERIC PROGRAMMING STANDARDS .....	58
PROGRAMMING STANDARDS ON THE ISERIES (RPG) .....	58
STANDARDS FOR WINDOWS AND WEB BASED PROGRAMMING .....	60
PROMOTION OF CODE .....	62
<b>DOCUMENTATION .....</b>	<b>62</b>
STANDARD USER DOCUMENTATION .....	62
STANDARD SYSTEM DOCUMENTATION .....	62
<b>APPENDIX A – PROJECT PLAN MODEL .....</b>	<b>63</b>
<b>APPENDIX B .....</b>	<b>64</b>
NOTE: THE TIME COST IS TO BE CALCULATED BASED ON \$75 PER HOUR PER PERSON FOR IT PERSONNEL AND \$50 PER HOUR PER PERSON FOR NON-IT PERSONNEL	64
<b>INSIDER THREAT POLICY .....</b>	<b>64</b>
<b>INCIDENT RESPONSE POLICY .....</b>	<b>66</b>
TYPES OF INCIDENTS .....	66
AUTOMATED SYSTEMS FOR SUPPORT WITH INCIDENT HANDLING .....	67
LEGAL AND SLA INCIDENT REPORTING REQUIREMENTS .....	67
INCIDENT REPORTING OUTSIDE GATESTONE & CO. ....	68
INCIDENT RESPONSE ROLES AND RESPONSIBILITIES .....	68
EXECUTIVES .....	68
USERS .....	68
HELP DESK .....	68
SECURITY OFFICER .....	68
SYSTEMS ADMINISTRATOR .....	69
NETWORK ADMINISTRATOR .....	69
INCIDENT RESPONSE TEAM .....	69
TEAM MEMBERS .....	69
EVIDENCE HANDLING .....	69
CLEAR CHAIN OF CUSTODY: .....	69



WEIGHT OF EVIDENCE: ALL EVIDENCE WILL BE COLLECTED IN AN IMPARTIAL MANNER.  
..... 70

EVIDENCE GATHERING: PHOTOGRAPHS, LOGS, HARDWARE (LAPTOPS, PDA'S ECT) 70

**E-MAIL INTERNET AND ACCEPTABLE USE POLICY.....72**

**SEPARATION/ SEGREGATION OF DUTIES.....73**

EXPLANATION..... 73

PROCEDURE ..... 73

**ROLES AND RESPONSIBILITIES .....74**

EXECUTIVES..... 74

BUSINESS PERSONNEL..... 75

SUPPORT PERSONNEL (NON-IT)..... 75

INFORMATION & TECHNOLOGY ..... 76

**SIGN OFF.....78**

I.T. DEPARTMENT ..... 78

**APPENDIX A – BASIC SECURITY CONCEPTS .....79**

CONFIDENTIALITY..... 79

INTEGRITY ..... 79

AVAILABILITY..... 79

AUTHENTICATION, AUTHORIZATION, AND NON-REPUDIATION..... 79

**PRIVACY .....80**

**CLEAN DESK POLICY .....80**

**PCI COMPLIANCE POLICY.....80**

**APPENDIX B – TYPES OF SECURITY INCIDENTS .....81**

PROBE ..... 81

SCAN ..... 81

ACCOUNT COMPROMISE..... 81

ROOT COMPROMISE..... 81

PACKET SNIFFER..... 82

DENIAL OF SERVICE..... 82

EXPLOITATION OF TRUST ..... 82

MALICIOUS CODE..... 82

INTERNET INFRASTRUCTURE ATTACKS ..... 82

**APPENDIX C - ANATOMY OF A SECURITY POLICY .....83**

SECURITY POLICIES ..... 83

SECURITY-RELATED PROCEDURES ..... 83

SECURITY PRACTICES ..... 83

INTRUSION DETECTION..... 84

## Executive Summary

---

It is remarkably easy to gain unauthorized access to information in an insecure networked environment, and it is hard to catch the intruders. A robust defence requires a flexible strategy that allows adaptation to the changing environment, well-defined policies and procedures, the use of robust tools, and constant vigilance. Integral to a security program are documented policies, procedures, and practices, and regular reviews and audits.

This security policy shall be reviewed, modified and agreed upon by the managers of the organization annually and distributed to each employee, at the time of hire, and any time a revision is made.

## Information Security Team members

---

Nicholas Wilson	Chairman and Chief Executive Officer
John Tilley	President
Nicholas Dowd	Executive Vice President and Chief Financial Officer
Claude LaPointe	IT director
Suzanne Huether	Manager, Human Resources
Robert Coats	Information Security Officer
Nilda Mejias	Manager, Computer Operations

Please refer to the Corporate Intranet for contact information

## POLICY CREATION GUIDELINE

---

Creating policy for Gatestone & Co. will pass through a process of evaluation and approval, which will ensure proper support of all parties, affected. Policy will pass through Gatestone & Co. change control process and gain approval at highest level. All these Policy and procedure will pass through an annual review and approval to ensure policies are up to date. This policy and change changes will be published on the Gatestone Intranet for all employee's to read. They users will be required to accept the changes on the Intranet on a yearly basis.

## Acceptable Use Policy

---

The purpose of this policy is to outline the acceptable use of computer equipment at Gatestone & Co. These rules are in place to protect the employee and Gatestone & Co. Inappropriate use exposes

Gatestone & Co. to risks including virus attacks, compromise of network systems and services, and legal issues. This policy applies to employees, contractors, consultants, temporaries, and other workers at Gatestone & Co. including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Gatestone & Co.

#### Monitoring of Employees

Authorized Gatestone & Co. employees may monitor equipment, systems, email, Internet access, and network traffic at any time for security, and network maintenance purposes. Gatestone & Co. reserves the right to use automated tools and cameras to monitor any or all movement and communications inside Gatestone & Co. offices.

#### 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). Under no circumstances is an employee of Gatestone & Co. authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Gatestone & Co. owned resources. The list below is by no means exhaustive, but an attempt to provide a framework for activities, which fall into the category of unacceptable use.

- 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 Gatestone & Co.
- 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 Gatestone & Co. or the end user does not have an active license is strictly prohibited.
- Its prohibited to use photographic, video and audio recordings to capture client data.
- 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.
- Installing or using software or programs that have not been authorized by the Corporate Security Officer and Senior management.
- Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Wireless peripherals are prohibited from being used with the exception of wireless mice.
- Personally owned mobile devices will not be connected to Gatestone equipment for any reason (including charging)
- 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.
- Using a Gatestone & Co. computing asset to actively engage in procuring or transmitting illegal or banned material.
- 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.

- Port scanning or security scanning is expressly prohibited, unless this activity is a part of the employee's normal job/duty.
- Executing any form of network monitoring, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user of Gatestone & Co. (for example, denial of service attack).
- 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.
- Providing information about, or lists of, Gatestone & Co. employees to parties outside Gatestone & Co.
- 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).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- 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.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

## **EXCEPTION TO POLICY**

---

In order to continue with business as usual (BAU), policies must be adhered to. If a member, department or remote office deems the policy interferes with BAU an "Exception to Policy" request may be warranted. Exceptions to policy requests are unique in nature and will be considered on a case-by-case basis. Justification is the key to all requests. An exception form is to be filled out and signed by the senior VP of that division asking for the exception to policy with the reason for the request. The security officer will review and grant the request after a security assessment and thoroughly document the exception for annual review.

Requests for exception must include: a valid business justification; a risk analysis; compensating controls to manage risk; and technical reasons for the exception.

Requests for exception that create significant risks without compensating controls will not be approved.

Request for exception will need approval from the security officer and senior VP of division.

Requests for exceptions must be periodically reviewed to ensure that assumptions or business conditions have not changed. Exemption renewals are not automatically approved.

\*Any exception to policy that affects client data will require confirmation and approval in writing first from the client in question. Currently this requirement is for a client.

### **Visitors Access Policy**

---

1. When a visitor enters Gatestone & Co. reception, they must advise: who they are, what business they are transacting and whom they are meeting.
2. Reception must verify visitors with photo ID, such as a driver's license. They must then call the person whom the visitor is here to see and ask them to approve of the visitor and then to come to reception to sign for them.
3. The visitor must be signed into a log book detailing: their name, date, Gatestone & Co. contact, the company they represent, their visitor Badge number and the nature of the visit.
4. Once the Gatestone & Co. contact has arrived at reception and signed in for the visitor, a visitors badge must then be issued to the visitor to wear at all times. Visitor badges have no access rights to the physical door security. NOTE : Upon VP approval some badges will be given access to the Operations area, all Visitors will be escorted by a Gatestone employee
5. The Gatestone & Co. must be escorted at all time and are not allowed entry into departments/rooms unrelated to the visit. This includes listening to calls and viewing workstations not directly related to their business.
6. Visitor badges must be returned to reception at the end of the day. The Gatestone & Co. contact must then sign the visitor out and escort them to the elevators.
7. At end of day, Reception verifies all visitors have been signed out and that all badges have been returned. If not, Reception contacts the Gatestone & Co. employee responsible for the visitor.
8. The Gatestone & Co. contact verifies that the visitor is still in the building. If after hours, they will retrieve the badge, escort the visitor from the premises and return the badge to reception the next day.
9. The Gatestone & Co. contact verifies the visitor has left the premises. They return to reception to resolve the issue of either a) Badge not returned or b) Forgot to sign out the visitor. The issue is logged and reviewed.
10. Log of kept for a period of 6 months.

## Access Control Policy

---

### Summary

- Customer information is categorized as sensitive and restricted.
- Customer information is confidential and must be protected. The Family Educational and Rights and Privacy Act (FERPA), Personal Information Protection and Electronic Documents Act (PIPEDA), Personal Information Protection Act (PIPA) and the Gramm-Leach-Bliley Act (GLBA) specify obligations that Gatestone & Co. must fulfil with respect to information security.
- All requests for administrative system account activity (adds, changes, or deletions) must be submitted via email to [OPS@Gatestone&CO.com](mailto:OPS@Gatestone&CO.com).
- Every employee must access the system using his or her assigned user id and password. Passwords must NEVER be shared for any reason.
- The Operations Department and the Security Administrator are responsible for authorizing and monitoring access to the system and they must promote this policy and assist users in their area with understanding the appropriate use of information resources.
- Users will automatically be logged out of Iseries sessions after 30 minutes of inactivity.
- All systems will have a security Banner in place detailing the following.
  - That the user is accessing Gatestone & Co. information system;
  - That system usage may be monitored, recorded, and subject to audit;
  - That unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
  - That use of the system indicates consent to monitoring and recording
- Employees/contractors granted access to data might do so only for business. In this regard, employees must:
  - Respect the confidentiality and privacy of individuals whose records they access
  - Sign and acknowledge the Non-disclosure agreement.
  - Sign and acknowledge the Information security policy
  - Ensure the encryption controls
  - Observe ethical restrictions that apply to the data to which they have access
  - Abide by applicable laws or policies with respect to access, use, or disclosure of information.
- Employees/contractors must not:
  - Disclose data to others, except as required by their job responsibilities
  - Use data for their own personal gain, nor for the gain or profit of others
  - Access data to satisfy their personal curiosity
- Contractors : who have access to client data for business purposes will
  - Will be monitored at all times when access to sensitive information is available.
  - We will have the vendor sign a attestation stating they are leaving without customer information
  - Access lists will be reviewed quarterly by the security officer based on theory of least privilege remove unneeded Access will be removed immediately after contractors are complete. Employees who violate this policy are subject to investigation and disciplinary procedures of Gatestone & Co.

#### New employees/Contractors:

1. Human Resources or their representative provides a written copy of the Security Policy and confidentiality to the new employee/contractor.
2. The employee/contractor signs the Security Policy and the Confidentiality Agreement.
3. H.R. must send an email to **OPS@Gatestone& Co.com** and to the Vice President to whom the new employee or contractor will report, a list of new employees/contractors indicating:
  - a. Employee/contractors first and last name.
  - b. Employee/contractors hired position.
  - c. Department
  - d. Supervisor
  - e. Vice President
  - f. Client Access Requirement
4. The Vice President to whom the new employee/contractor will report must then send an e-mail to [OPS@Gatestone& CO..com](mailto:OPS@Gatestone& CO..com) approving access to the appropriate client data for that employee.
5. System Administrator creates the login and assigns the appropriate security classes (refer to the Password and authentication policy) within one business day. The system administrator will update the list of new employees/contractors adding the following information:
  - a. User Ids (LAN and AS400) if needed
  - b. Email address, if it is needed.
6. System Administrator will email the list of new employees/contractors ID's to:
  - a. H.R.
  - b. Compliance
  - c. Training
  - d. The Vice President to whom the new employee(s) will report.
7. Passwords are sent to the manager and trainer of the department via secure email.
8. Human resources or local admin creates the badge for the employee or contractor to gain access to the required site/sites.
9. Badge is to be worn at all time in a visible way
10. Employees are required to conduct security awareness training at start of their work and yearly after that.
11. Contractor user ID's will be reviewed monthly to confirm appropriate access rights monthly.

#### Terminated or resigning employees/contractors:

1. Managers or their representative must send a request to the Help Desk disable the employees or contractors user id on the LAN and AS400 immediately after notifying the employee or contractor of the decision to terminate or change of roles of his/her with Gatestone & Co. or immediately after receiving the employee's/contractors resignation letter (if the employee will leave right away) or at the end of the last working day.
2. Client service rep will inform the client of the termination if required by the SLA

3. Supervisors must send an email to the Help Desk and to H.R. advising the termination or change of roles of the employee's or contractors contract immediately after the termination or role change, indicating:
  - a. Employee first and last name.
  - b. Employee user id.
4. H.R. will deactivate the access card for the terminated employee or contractor and follow their termination procedure.
5. H.R. must send the list of terminated or resigning employees to [OPS@Gatestone&CO..com](mailto:OPS@Gatestone&CO..com). Equipment is collected and the termination procedure is followed.
6. The security administrator will remove access privileges from all the users in the list and confirm that the employee's access card has been disabled.

#### Other users' maintenance (Promotions, transfers, Contractors etc.)

1. Supervisors must request any changes to the user ids to the Help Desk via email.
2. Changes will be implemented immediately.
3. H.R. will update the users on the AS400 to add the applicable state/province to the collector user's id when the provincial collector's license is received.
4. Upon completion of the contract the user ID will be disabled.

#### Building employees

HR will request building to conduct a background check on all employees who have access to Gatestone & Co.'s premises. Staff failing this access will not be allowed to enter Gatestone & Co.'s premises.

#### Hiring Policy

---

Gatestone & Co.'s Hiring policy requires that all candidates selected for an interview be pre-screened by a skilled Human Resources representative who will evaluate the candidate's job and cultural fit to the organization.

During the Pre-screening process candidates complete the Personality Index and receive an interview. The personality index is an advanced behaviour and personality profiling system that measures behaviour traits and identifies top performers.

The pre-screen interview further assesses the candidate evaluating communication skills and prior experience. If successful, the candidate receives a second interview by the line manager. The Line manager recommends to HR their final candidate choice, a conditional offer letter, subject to successful completion of background screening, is presented to the candidate. All new hires must complete a



criminal record check and references to continue employment with the company. Drug testing is not completed in any Canadian centre due to Human Rights legislation reasonable cause issues.

#### Access auditing and entitlement review

On a periodic basis, the System Administrators will review reports identifying failed login attempts, “super user” logins and origins of login.

Every 30 days a review of the highly sensitive area’s will be conducted which includes all access to computer rooms . This will be recorded on a monthly checklist.

Semi-annually, the System Administrator will be required to review a complete list of all system privileges assigned in their area. The cover page of this report must be signed by the IT Department.

#### Enforcement

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

## Anti-Virus Policy

---

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. Computers with detected viruses will be removed from the network immediately. It must be freshly installed before being allowed on Gatestone's network. Home PC's will not be connected to our network for any reason.

- Always run the corporate standard and supported anti-virus software is available from helpdesk. Do not change, or attempt to change the default anti-virus software settings as supplied by help desk.
- Virus definition files will automatically be updated to all servers and desktops when available.
- All Desktops will be set to auto protect and to randomly scan for undetected viruses.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Never run any programs sent to you via email or downloaded from the Internet that end with the extension .exe or .vb\* without express permission from helpdesk.
- Delete spam, chain, and other junk email without forwarding, in with Gatestone & Co. *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with other users unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Anti-virus Software will be monitored on all workstations for compliance.
- If Virus or malware is detected it is removed immediately and recorded.
- Remediation of workstations and EPO monitor will be conducted every 30 days to confirm compliance.

## Audit Policy

---

This policy covers all computer and communication devices owned or operated by Gatestone & Co. This policy also covers any computer and communications device that are present on Gatestone & Co. premises, but which may not be owned or operated by Gatestone & Co.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents ensure conformance to Gatestone & Co. security policies
- Monitor user or system activity where appropriate.

When requested, and for the purpose of performing an audit, any access needed will be provided to members of Gatestone & Co.'s systems management team. The Systems management group will run audits once per year with internal quarterly reviews.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced transmitted or stored on Gatestone & Co. equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to monitor and log traffic on Gatestone & CO. networks.

Continual auditing by the event-logging operator of the following events for 120 days will ensure a construction of events. These events will be reviewed daily for anomalies and escalated to the incident response team. These audit logs will have frequency and scope changed when an increased potential for harm is envisioned or is requested by law enforcement/client. Local and network administrators will not have change access to these logs and storage of this database of logs will be held in a physically secure manner with limited access to the event logging operator only.

- Change in access for groups and individuals
- Locked passwords
- Access to critical files. All files that contain critical client data will have all types of access logged for future reference. This includes modify, delete, copy and read.
- IDS logs
- Firewall logs
- Badge access logs

## Security Assessment and Certification

---

### Explanatory Note:

The policies associated with Security Certification and Accreditation is intended to:

- Ensure that security controls identified in requirements and design stages have been developed, tested, and are operational prior to the implementation of new or significantly enhanced information systems, information services or information processing facilities.
- Ensure that management makes informed decisions on the adequacy of security controls when granting Accreditation.
- Reinforce the need to include Security Certification and Accreditation processes into acceptance criteria and procurement documents.
- Ensure that processes for making changes to systems, services and facilities include Security Certification and Accreditation requirements.
- Ensure that information is suitably protected from threats to confidentiality, integrity and availability.

### Requirements of all changes

- Report Implementation of new or significantly changed information systems, services or facilities, which have not received Accreditation.
- Report Actual and suspected security incidents and events as required by policies and processes.
- Ensure systems acceptance criteria are documented during the requirements phase of the systems development lifecycle.
- Complete training on new or significantly changed systems prior to implementation.
- Ensure that information in this policy is disseminated to all employees at Gatestone & Co.

### Requirement of management:

- Prior to granting Accreditation ensure that residual risks are within predetermined tolerance levels.
- Ensure personnel roles and responsibilities are clearly defined.
- Ensure personnel have received adequate training on new systems or services prior to implementation.
- Ensure Certification and Accreditation tasks are conducted by qualified personnel. Contact information security officer for details.
- Update and test contingency plans and disaster recovery plans when required by a Security Threat and Risk Assessment prior to granting Accreditation.
- When a security or privacy breach has occurred, review and revise related policies and processes as needed.
- Deficiencies identified in Security Certification reports are mitigated or accepted.

### Asset Control

---

- An inventory will be kept for all assets held by Gatestone & Co.
- Assets of a portable nature will be labelled as "Gatestone & Co. Property please return to helpdesk at 180 Duncan Mill, Toronto On, M3B 1Z6 if found"
- IT assets lent out to any employee must be approved by their manager via the appropriate forms and signed off by the operations manager. The form will be held in a safe location for future reference.
- It assets returned will be reviewed for security threats. I.E Key loggers, Unknown attached devices, non-approved software, and viruses. Escalate to incident team as appropriate.
- Annual asset inventory of all software and hardware will be completed once per year. This will include the licenses for software.
- Assets will be identified by a unique serial number or asset control tag.

## Information Sensitivity Policy

---

### Security and Proprietary Information

Users should be aware that the data they create on the corporate systems remains the property of Gatestone & Co. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Gatestone & Co. without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

### Classification of Information

All Gatestone & Co. information is categorized into two main classifications:

- Gatestone & Co. Non-Sensitive Sub divided into Public and Non Public.
- Gatestone & Co. Sensitive Sub divided into Critical and Restricted.

Gatestone & Co. Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Gatestone & Co.

Gatestone & Co. Non Public is Information which management believes requires limitations on internal access on a “need-to-know” basis, but which does not fall under the definition of “sensitive information”. This includes routine correspondence, employee newsletter, internal phone directories, in-office memoranda, internal policies, processes, guidelines, and procedures

Gatestone & Co. Sensitive information contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included are information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included is information that is less critical, such as general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

Gatestone & Co. Critical Information, which must be available in order for Gatestone & Co. to effectively perform its mission and meet legally, assigned responsibilities. Critical information requires that special precautions be taken to ensure its accuracy, relevance, timeliness, and completeness. This information, if lost, could cause significant financial loss, inconvenience, or delay in performance of Gatestone & Co.’s mission and a loss of public trust. This includes division financial data, purchasing information, vendor contracts, risk assessments, and internal auditing reports and findings.

Gatestone & Co. restricted information is any information that has limitations placed upon its internal access and that may be disclosed only in accordance with an executive order, public law, federal statute (HIPAA, GBL, Privacy Act of 1974, etc.), and supporting Gatestone & Co.'s policies, guidelines, procedures, and processes. This includes all client information, statutorily protected and sensitive information, and corporate information such as customer forms, corporate forms, strategic corporate plans/ financial information, employee records, employee health information, and investigation reports and finding.

Gatestone & Co. personnel are encouraged to use common sense judgment in securing Gatestone & Co. Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager.

Access to information and system resources such as equipment or programs is granted on a need to know or need to use basis. Access rights are specified by individual user or by groups of users. For example, users performing the same function on the same data are allocated to a group profile and access rights assigned to the group. Access to specialized functions is assigned on an individual basis. Audit trails are maintained for all activity on the system so that any event can be tracked to an individual user.

Refer the matrix below for specifics on how to handle information.

Client data will not be moved, copied or shared with anyone outside is secure domain without first contacting the client for approval.

Transport of information will be of an approved method following the classification matrix. The transport agency will be a bonded carrier with appropriate insurance.

NOTE: Users ID's and passwords are classed as Sensitive Restricted information and are never to be shared with anyone except senior staff for troubleshooting purposes.

### Data and Media Classification and Protection Matrix

Non Sensitive		Sensitive	
Public	Non Public	Critical	Restricted

<b>Examples</b>	Brochures, news releases	Routine correspondence, employee newsletter, internal phone directories, in-office memoranda, internal policies, processes, guidelines, and procedures	Division financial data, purchasing information, vendor contracts, risk assessments, and internal auditing reports and findings.	Statutorily protected and sensitive information, / corporate information such as: customer forms, corporate forms, strategic corporate plans/ financial information, employee records, employee health information, and investigation reports and finding.
-----------------	--------------------------	--	--	--

<b>Criteria</b>	Information, which can be made available to anyone without exception. It is neither sensitive nor controlled.	Information which management believes requires limitations on internal access on a "need-to-know" basis, but which does not fall under the definition of "sensitive information".	Information, which must be available in order for Gatestone & Co. to effectively perform its mission and meet legally, assigned responsibilities. Critical information requires that special precautions be taken to ensure its accuracy, relevance, timeliness, and completeness. This information, if lost, could cause significant financial loss, inconvenience, or delay in performance of Gatestone & Co.'s mission and a loss of public trust.	Restricted mandatory information is any information that has limitations placed upon its internal access and that may be disclosed only in accordance with an executive order, public law, federal statute (HIPAA, GBL, Privacy Act of 1974, etc.), and supporting, and Gatestone & Co.'s policies, guidelines, procedures, and processes.
<b>Handling Standards</b>	No Special handling required.	No Special handling required.	Encryption is required when sending information over an untrusted network i.e., the Internet or non-secure email system. When sensitive information is commingled with non-sensitive information through computer processing and merging of data or insertion of documents files, the resulting file, tape, or disk which contains the commingled data must be clearly labelled that "Sensitive information is Included.	Encryption is required when sending information over an untrusted network i.e., the Internet or non-secure email system. When sensitive information is commingled with non-sensitive information through computer processing and merging of data or insertion of documents files, the resulting file, tape, or disk which contains the commingled data must be clearly labelled that "Sensitive information is Included.
<b>1. Release to 3<sup>rd</sup> party</b>	Available to the general public and for distribution outside of the Gatestone & Co.	Intended for use only within the Gatestone & Co. May be shared outside the Gatestone & Co. only if there is a legitimate business need to know, and is approved by the data owner and users manager.	Access limited to as few persons as possible on a need to know basis. Information is very sensitive and closely monitored using auditing tools. Information is controlled from creation or acceptance to destruction or return of information. Release only permitted by appropriate policies and procedures.	Access limited to as few persons as possible on a need to know basis. Information is very sensitive and closely monitored using auditing tools. Information is controlled from creation or acceptance to destruction or return of information. Release only permitted by appropriate policies and procedures.

<p><b>2. Transmission by Post, Fax, Email standards</b></p> <p>a. Mail within the organization (interoffice).</p> <p>b. Mail outside of the organization</p> <p>c. E-mail within the organization</p> <p>d. E-mail outside of the organization</p> <p>e. FAX</p> <p>1). Location of fax machine.</p> <p>2). Use of fax coversheet.</p> <p>3). Transmission safeguards.</p>	<p>a. No special handling required.</p> <p>b. No special handling required.</p> <p>c. No special handling required.</p> <p>d. No special handling required.</p> <p>1). Located in area not accessible to general public.</p> <p>2). Required.</p> <p>3). Reasonable care in dialling.</p>	<p>a. No special handling required. b. 1st class mail. No special handling required.</p> <p>c. No special handling required.</p> <p>d. No special handling required.</p> <p>1). Located in area not accessible to general public.</p> <p>2). Required.</p> <p>3). Reasonable care in dialling.</p>	<p>a. Sealed inter-office envelope marked and labelled "sensitive Information". Notify recipient in advance.</p> <p>b. 1st class USPS mail. Traceable delivery required, e.g. messenger, FedEx, U.S. express, USPS certified, or return receipt mail.</p> <p>c. Use of e-mail strongly discourage unless encrypted.</p> <p>d. Use of e-mail strongly discouraged unless encrypted</p> <p>1). Located in area not accessible to general public and unauthorized persons.</p> <p>2). Required. Coversheet</p> <p>3). Telephone notification prior to transmission and subsequent telephone confirmation of receipt required.</p>	<p>a. Sealed inter-office envelope marked and labelled "sensitive Information". Notify recipient in advance.</p> <p>b. 1st class USPS mail. Traceable delivery required, e.g. messenger, FedEx, U.S. express, USPS certified, or return receipt mail.</p> <p>Use of e-mail strongly discourage unless encrypted.</p> <p>d. Use of e-mail will be encrypted</p> <p>1). Located in area not accessible to general public and unauthorized persons.</p> <p>2). Required. Coversheet</p> <p>3). Telephone notification prior to transmission and subsequent telephone confirmation of receipt required.</p>
<p><b>3. Transmission by Spoken word</b></p> <p>a. Conversation/ Meetings</p> <p>b. Telephone</p> <p>c. Cellular Telephone</p> <p>d. Lobby announcement</p> <p>e. Overhead pages</p>	<p>No special precautions required.</p>	<p>Reasonable precautions to prevent inadvertent disclosure.</p>	<p>Active measures and close control to limit information to as few persons as possible.</p> <p>a. Enclosed meeting area. Public areas prohibited.</p> <p>b. Avoid proximity to unauthorized listeners. Speakerphone in enclosed area. Use generally discouraged.</p> <p>c. Use of digital telephones discouraged, landline preferred.</p> <p>d. No Lobby announcements.</p>	<p>Active measures and close control to limit information to as few persons as possible.</p> <p>a. Enclosed meeting area. Public areas prohibited.</p> <p>b. Avoid proximity to unauthorized listeners. Speakerphone in enclosed area. Use generally discouraged.</p> <p>c. Use of digital telephones discouraged, landline preferred.</p> <p>d. No Lobby announcements.</p>
<p><b>4. Print, Film, Fiche, Video</b></p> <p>a. Printed Materials</p> <p>b. Sign-in sheets/Signin</p>	<p>No special precautions required.</p>	<p>Reasonable precautions to prevent inadvertent disclosure.</p> <p>a. Store out of sight of none employees.</p>	<p>Active measurers and close control to limit information to as few persons as possible.</p>	<p>Active measurers and close control to limit information to as few persons as possible.</p> <p>a. Store out of sight in a lockable enclosure.</p>



<p>Logs c. Monitors/Computer Screens</p>		<p>b. Placement out of sight of non-employees. c. Positioned or shielded to prevent viewing by nonemployees.</p>	<p>a. Store out of sight in a lockable enclosure. b. Subsequent signers cannot identify signer. c. Position or shield to prevent viewing by unauthorized parties. Possible measurers include: physical location in secure area, positioning of screen, use of password screen saver, etc.</p>	<p>b. Subsequent signers cannot identify signer. c. Position or shield to prevent viewing by unauthorized parties. Possible measurers include: physical location in secure area, positioning of screen, use of password screen saver, etc.</p>
<p><b>5.Copying Standards</b></p>	<p>No special precautions.</p>	<p>No special precautions.</p>	<p>Photocopying with approval by Data Owner. (Note: If a digital copier is used, cache needs to be erased.)</p>	<p>Photocopying with approval by Data Owner. (Note: If a digital copier is used, cache needs to be erased.)</p>
<p><b>6.Storage Standards</b></p> <p>a. Printed Material b. Electronic documents c. E-mail</p>	<p>a. No special precautions required. b. Storage on all drives. c. No special precautions required.</p>	<p>a. Reasonable precautions to prevent access by non-employees. b. Storage on all drives. c. Reasonable precautions to prevent access by unauthorized personnel.</p>	<p>a. Storage in a lockable enclosure. b. Storage on secure drives only. Password protection of document preferred. Reuse to erase sensitive information by over writing 7 times or destruction of drive c. Encrypted storage and backup tape in a secure place or container.</p>	<p>a. Storage in a lockable enclosure. b. Storage on secure drives only. Password protection of document preferred. Reuse to erase sensitive information by over writing 7 times or destruction of drive. c. Encrypted storage and backup tape in a secure place or container.</p>
<p><b>7.Destruction Standards</b></p> <p>a. Destruction b. Location of waste paper bins. c. Paper recycling. d. Magnetic Media/disks which include As400, servers, workstations and laptops.</p>	<p>a. No special precautions required. b. No special Precautions required. c. Permitted. d. No special precautions required.</p>	<p>a. No special precautions required. b. No special Precautions required. c. Permitted. d. No special precautions required.</p>	<p>a. Destroy in a manner that protects sensitive information. b. Secure area not accessible to unauthorized persons. c. Prohibited. Destruction or shredding required. d. Physical destruction with a witness and certificate of destruction</p>	<p>a. Destroy in a manner that protects sensitive information. b. Secure area not accessible to unauthorized persons. c. Prohibited. Destruction or shredding required. d. Physical destruction with a Witness and certificate of destruction</p>
<p><b>8.Physical Security</b></p> <p>a. Computer/ Workstations b. Printing Documents c. Office Access d. Laptop, Palm, etc.</p>	<p>a. Password screen-saver to be used when briefly unattended. Sign-off or power-off work stations or terminals when not in use or leaving work. b. No special precautions required.</p>	<p>a. Password screen-saver to be used when briefly unattended. Sign-off or power-off work stations or terminals when not in use or leaving work. b. No special precautions required. c. No special precautions required.</p>	<p>a. Do not leave data unattended. Sign-off, Lock or power-off workstation/terminals not in use or leaving work area. b. Printing of documents when necessary must not be left unattended. The person attending the</p>	<p>a. Do not leave data unattended. Sign-off, Lock or power-off workstation/terminals not in use or leaving work area b. Printing of documents when necessary must not be left unattended. The person attending the printer must</p>

	<p>c. No special precautions required.</p> <p>d. No special Precautions required.</p>	<p>d. No special Precautions required.</p>	<p>printer must be authorized to examine the sensitive information being printed.</p> <p>c. Access to areas containing sensitive information should be physical restricted. Sensitive information must be locked when left in an unattended room.</p> <p>d. Computer must not be left unattended at any time unless the sensitive information is encrypted or the hardware is secured in a locked file cabinet, room, or safe.</p>	<p>be authorized to examine the sensitive information being printed.</p> <p>c. Access to areas containing sensitive information should be physical restricted. Sensitive information must be locked when left in an unattended room.</p> <p>d. Computer must not be left unattended at any time unless the sensitive information is encrypted or the hardware is secured in a locked file cabinet, room, or safe.</p>
<b>9. Access Control</b>	Available to the general public.	Generally available to all authorized users on a need to know basis.	Must have a business, need to know the information. Must have written approval of the data owner.	Must have a business need to know the information. Must have written approval of the data owner.
<b>10. Audit Standards</b>	None	None	Access shall be granted by the data owner and audited.	Access shall be granted by the data owner and audited.

Penalty for deliberate or inadvertent disclosure:

Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

### Labeling Policy

- All documents will have a title page that clearly states the data owner, Level of Confidentiality, Revision level of the document and authorization of change
- All documents are to have a footnote on every page indicating the owner and classification of the document
- Where printing provides, documents will have a watermark labelled across it stating the classification of the document.
- Hardware that stores or transports information will have labels indicating its classification.
- Hardware will not have labels indicating the exact nature of the information or any identifying marks indicating client names. They can be labelled with coded references to clients.

## Availability controls

---

- Information owners or Business personnel are responsible for ensuring contractual compliance between clients. New requirements will be brought through Gatestone & Co.'s change control process before implementation.
- Compliance department will be responsible for ensuring legal availability requirements on all information. New requirements will be brought through Gatestone & Co.'s change control process for implementation
- IT department will monitor and ensure processes and equipment is good working order. Procedures will be written down and real time monitoring will be conducted on all processes.
- Availability controls are subject to the security policies of this document.

## Present Controls

- Critical information is to be backed up daily and stored remotely for historic recovery.
- Information deemed critical to be replicated to at least 1 remote location. Presently our main database, FTP and user information will be replicated. All other information will be backed up daily.

Hardware: Network infrastructure essential for business continuity will have identical set up and equipment at the backup office.

- Firewall/Internet: Identical bandwidth and policy will be available at each backup location
- Phone Switch: Capacity at each backup location will allow dial tone and calling without being dependant on any other location.
- Email: Will be replicated offsite to prevent loss of information and will allow remote access from the Internet.

Legal Requirements: Gatestone & Co. will meet the following requirements pursuant to legal requirements or changes in policy.

- Email- Will be archived for 6 years
- Accounting information- Will be archived for 7 years
- Phone system - Daily translation backed up
- Backups: Daily, and weekly backups are kept until a month end has been verified. Month end tapes will be stored offsite and will not be re- used.

## Photographic and recording device policy

---

### PURPOSE:

Client confidential information shall not be stored or recorded on any portable device without the written consent of the client in question. If this is approved the data will follow the encryption policy mentioned in this policy document

For the purpose of securing all business related data; no recording and/or photographic equipment will be allowed in the facility. This policy refers to; but is not restricted to:

- Cameras of any type
- Cellular phones with recording/photographic capabilities
- Memory cards
- External storage devices \USB sticks\phones, CD-ROMs, laptops and notebooks.

Any use of these types of devices that will allow the recording, duplication and/or transportation of data outside of the Gatestone & Co. premises will not be allowed and may result in disciplinary actions.

## Risk Assessment Policy

---

### Mission Statement

***To empower Information Security Officer to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.***

### Explanatory Notes

Risk assessments can be conducted on any entity within Gatestone & Co. or any outside entity that has signed a *Third Party Agreement* with Gatestone & Co. RA can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

### Risk Assessment Requirements

- The execution, development and implementation of remediation programs is the joint responsibility of information security officer and the department responsible for the systems area being assessed.
- Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable.
- Employees are further expected to work with the Information Security Officer or his team in the development of a remediation plan.
- Risk assessment to be conducted on a bi-annual basis on all critical and sensitive information and annually on non-critical.
- All new processes will have a RA conducted on it to determine risk
- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

- RA will follow the Risk assessment procedure document Gatestone & Co. releases.

## Encryption Policy

---

### Encryption Mission Statement

***"Sensitive or confidential data / information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured e.g. by using encryption techniques." Information owners will agree upon confidentiality and encryption techniques and inform the information owner of all changes.***

### Explanatory Notes

The way in which your data is distributed across networks (both public and private) and by other means e.g. the exchange of tapes, disks, diskettes and optical disks (e.g. CD-ROMs). *Information Security issues to be considered when implementing your policy include the following:*

- Incorrect data released to outside parties can lead to a loss of confidence in the organization and / or its services.
- Any illegal amendment of / tampering with your data whilst in transit suggests a weakness that is being exploited.
- Where security measures have not been adequately deployed; unauthorized persons may access sensitive information.
- Confidential data may be distributed to inappropriate / unauthorized persons.
- The recipient of your data may have adopted Information Security standards, which are incompatible with yours. This constitutes a weak link in your security, which could be exploited.
- The inappropriate and possibly illegal release of information may result in legal action and prosecution.

### Encryption: Responsible parties

- Information security officer is responsible for policy and ensuring infrastructure procedures and processes are set up in a secure manner
- The user is responsible for using the encryption as intended and not to circumvent security procedure and or policy.
- Customer service rep for client is required to make sure they know the encryption requirements for their client and to inform the security officer if changes occur that process

### Encryption: Requirements

- All external communication of information deemed confidential (Incoming or Outgoing) will be encrypted. The transport and or the file will be encrypted as per client requirements. Currently ATT has this requirement.
- Encryption will follow all local and international laws governing its use. This includes international export/import rules.
- Voice recordings will be considered SPI data and will be encrypted in transit and at rest.
- Confidential information at rest will be encrypted. This includes tape storage, disk storage, optical storage, email archives and database storage.
- Encryption will always be required within the DMZ.
- All clients whose information is transported will agree upon encryption techniques and strengths. Gatestone & CO. will inform the client of any changes to encryption procedures.
- Email and or instant messages and similar correspondence will be encrypted
- Any encryption tools that are used will be maintained according to the server maintenance policy
- Data that is deemed confidential when at rest will be encrypted immediately accepted encryption practices.
- Keys will be at least 2048 Bit asymmetrical or 256 bit Symmetrical. The only 2 acceptable ciphers are AES and Quantum key distribution.
- Random number generation technique will follow NIST when used. Check publication SP800-90A.pdf for details.
- Check with PCI requirements to ensure not deprecated encryption techniques are used.

#### Encryption/Masking: Requirements credit card numbers:

- Masking of all credit card numbers is required if visible on the accounts list in Intellect. Preferably credit card numbers will not be sent and instead a reference number generated.

#### Encryption Key management

- Gatestone & CO. will always make a backup of encryption keys. If the encryption keys change, ensure that the changes are also backed up.
- Ensure that the backups are recoverable and effective during disaster recovery. Detail the recovery of these keys in documents and procedures
- Backup copies of the decryption keys will not be stored with the encrypted data
- Logical access control to our encryptions keys are for authorized users only in a physically and logically controlled server. Storing keys on the local drive or drives is prohibited.
- Keys no longer used will be destroyed in a safe and secure manner. This is either accomplished by over writing 7 times or destruction of the drive in question.

- Ensure that the key is only used and issued from a secure system. Ensure that the key generation process has high security and that the process has integrity.
- Ensure that keys are re-created on a yearly basis.
- Encryption keys will be changed if they are suspected of being compromised. Administrator left employment etc.

## **Password Authentication and Identification Protection Policy**

- Keep passwords secure. Account sharing is prohibited. Authorized users are responsible for the security of their passwords and accounts. Compromised usernames and passwords must be reported to the helpdesk immediately. System level passwords and user level passwords should be changed every 90 days. It is the responsibility of the Systems Manager to ensure that these standards are enforced.
- All passwords must be a minimum of eight letters and should not be the same as the user account.
- All programmatic account passwords are to have 14 characters in length.
- Passwords must include, at a minimum, two types of either letters, numbers, and special characters (e.g., #, !, %, etc.).
- Users will be required to change their initial password at first logon by first authenticating with page the current one.
- All passwords must be unique, defined as not being a password used in the last 12 months.
- Users will have one user profile to sign on onto the system. The user profile identifies the user accessing the system, and the objects the user is authorized to access or manipulate.
- Users are not permitted to sign on from multiple physical locations simultaneously.
- 3 invalid attempts to sign on to the network or the AS/400 will disable the user profile. Help desk can re-enable the profile on request.
- 5 invalid attempts to sign onto the network using active directory will result in a 15 minute lockout.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or less, or by logging-off (control-alt-delete for Window users) when the host will be unattended.
- Voice mail passwords must be unique and cannot be the phone extension number.
- Never divulge your password to anyone and change the password every 90 days.
- Passwords are not to be written down in clear text documents. Encryption of password documents is acceptable.
- Master passwords for each system are secured in the CIO 's office in a sealed envelope.
- Systems will uniquely identify and authenticate users and processes acting on behalf of users using either single or multifactor authentication as deemed necessary.
- Systems will obscure feedback of authentication information (e.g., display asterisks when a user types a password).
- Encryption will be used to protect passwords in both storage and transmission and will meet the requirements of Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules.

- CSOSA business and mission critical systems use either shared known information (e.g., Media Access Control (MAC) or Transmission Control Program/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks.
- Systems will lock after 5 minutes of inactivity requiring another password
- User will lock their devices when not in use.

### Service ID passwords

- Service ID's are ID's used for services or functions of an automated nature.
- Service ID's will follow the password procedure and policy rules stated here.
- ID's for service's will be consolidated in a record for analysis
- Service ID's will be the responsibility of the Information security officer follow the ID's lifecycle
- Service ID's will be disabled when no longer used and at 13 months whichever comes first

### Process Requirements

- Before a user can access the system:
  - The physical identity of the user will be verified.
  - The user will pass a background check completed by HR.
  - Human resources manager will request authorization from the departmental manager.
  - Upon receiving authorization, the System and/or IT Administrator will set up user profile based on information provided from the management department.
  - A unique user identifier will be issued to the user.
  - A temporary password will be created for the user.
  - The temporary password will be securely communicated to the user.
- New user identifiers will be maintained.
- Users will be placed in the client group they are working.
- An initial temporary password or a reissued temporary password will be changed the first time a user accesses business and mission critical systems.
- If a user forgets his/her password or believes it may have been compromised, he/she must report it to the IT Help Desk. Help Desk will verify the identity by requiring an email from the managing supervisor and matching this up with the user on the phone. Email must be from an internal source email.
- Upon notification that a user needs a new password, the System and/or IT Administrator will:



- Revoke the current password.
- Issue a new temporary password.
- Designate IT support personnel to review audit trails to investigate whether a breach has occurred.
- Inactive user identifiers will be disabled after 30 days.
- All default identifiers and authenticators will be changed.

### Roles and Responsibilities

A current list of roles and responsibilities will be maintained delineating responsibilities for executing, managing, monitoring and enforcing the procedures in this management instruction.

**Table I: Roles and Responsibilities**

<b>Roles</b>	<b>Responsibilities</b>
Chief Security Officer	<ul style="list-style-type: none"> <li>● Authorizes all administrator accounts.</li> </ul>
System Manager	<ul style="list-style-type: none"> <li>● Ensures Instruction technical and process controls are implemented.</li> </ul>
System Security Officer	<ul style="list-style-type: none"> <li>● Ensures Management Instruction procedures are implemented</li> <li>● Monitors compliance with policy</li> <li>● Ensures personnel are trained in operating and maintaining system controls.</li> <li>● Review audit records for inappropriate access related activities.</li> <li>● Ensure compliance with privacy policy</li> <li>● Investigate unusual activities.</li> </ul>
System Administrator	<ul style="list-style-type: none"> <li>● Assigns ID and initial Passwords to system users.</li> <li>● Assigns temporary passwords to users in the event a user forgets his/her password.</li> </ul>
IT Administrator	<ul style="list-style-type: none"> <li>● Assigns ID and Passwords to IT personnel who require administrator rights to system hardware and applications</li> </ul>
System users	<ul style="list-style-type: none"> <li>● Adhere to identification and authentication requirements as reflected in the employee handbook and Gatestone &amp; Co. security Policy.</li> </ul>

### Account Review Policy

---

- The system manager is responsible for reviewing a report of user activity every week.
- Any User account that has not been active in the past 60 days must be disabled. This is a system function that is run daily.
- Any account that has been disabled for 90 days must be deleted from the system. It is the responsibility of the Systems Manager to ensure that this standard is enforced.
- The system manager is responsible for reviewing the unauthorized attempts report every day. The system manager will investigate incidents reported on this report.
- User Accounts will be reviewed Bi-annually and access to systems restricted to least privilege to do their job.

### Router Security Policy

---

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of Gatestone & Co. All routers and switches connected to Gatestone & Co. production networks are affected.

Gatestone & Co.'s network will be protected from unauthorized access at all times by a systems management approved firewall where necessary.

Every router must meet the following configuration standards:

- No local user accounts are configured on the router. The enabled password on the router must be kept in a secure encrypted form. The router must have the enabled password set to the current production router password from the router's support organization.
- Disallow the following:
  - a. IP directed broadcasts
  - b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
  - c. TCP small services
  - d. UDP small services
  - e. All source routing
  - f. All web services running on router
- Use corporate standardized SNMP community strings.
- Access rules are to be added as business needs arise.
- The router must be included in the corporate enterprise management system with a designated point of contact.

## Network Security Policy

---

### Cable installation and management procedures

This section describes policy you will follow when installing LAN and switch cables. The objectives of these procedures are to:

- Provide switch cables with continuous support and strain relief
- Minimize the possibility of pin damage to the SNI ports
- Form consistent cable groups that comply with EMC certification
- Maintain efficient cooling
- Provide for a secure environment

#### Installation:

- Frames and support for all cables are required for proper security
- Cable routed in insecure locations will be placed in conduit.
- Separate cables into groups for nodes. Each node corresponds to a section of desks on the floor.
- Make certain cables do not run near interference sources (Electrical or Magnetic sources)
- Make certain that the cable bend radius does not exceed the cable standard.
- Connect only active users to the network and record the ports/desks used.

#### Management:

- Changes in active ports/desks are to be recorded in our Track it database and dated as to when the work was completed.
- All ports not in use are to be disconnected from the network.
- End users do not move network equipment. Only Helpdesk staffs are to move network equipment.

## Server and workstation Security and Maintenance Policy

---

The purpose of this policy is to establish standards for the base configuration of internal server and workstation equipment that is owned and/or operated by Gatestone & Co. Effective implementation of this policy will minimize unauthorized access to Gatestone & Co. proprietary information and technology. This policy applies to server equipment owned and/or operated by Gatestone & Co., and to servers registered under any Gatestone & Co.-owned internal network domain.

### Ownership and Responsibilities

An operational group that is responsible for system administration must own all internal servers deployed at Gatestone & Co. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by systems management. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by systems management.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Workstations must be registered with the enterprise management system. At a minimum the following information is required.
  - Workstation contact and location
  - Hardware and the operating System/Version
  - Main function and applications installed.
- Configuration changes for production servers and workstations must follow the appropriate change management procedures.
- System accounts that are needed will only be used for the functions specified by the software. They will not be used for logging in to do day to day administration. Users are to use their own ID to accomplish these tasks.

### **Chief Information Officer (CIO) shall:**

Establish a Center maintenance policy that implements the above policy and  
Maintain oversight of the maintenance policy implementation by the system information owners.

### **The Information System Owner or administrator shall:**

Implement the organization's system maintenance policy and use them to assess the system's Maintenance security controls. This is the only individual who makes changes to the system.

### **The information Security Office shall:**

Annually review, and update as required, the System Maintenance Policy and Procedures as part of the annual review of policy providing management oversight to assure compliance.

Annually certify maintenance policy to assure it satisfies the purpose, scope, and compliance requirements for system maintenance

#### General Configuration Guidelines

- Operating System configuration should be in accordance with approved systems management guidelines.
  - Only one operating system installed per server or desktop.
  - NTFS is used for all files systems.
  - Registry settings must be reviewed and set to acceptable guidelines as provided by systems management.
  - Auditing must be enabled on all servers according to guidelines provided by systems management.
  - No Modems are to be set up on any Server or workstation.
  - Firewall will be enabled and set up with minimum numbers of ports and IP's to be functional
  
- Services and applications that will not be used must be disabled where practical.
- Default passwords will be changed before the equipment goes into production.
- Default ID's will be changed before equipment goes into production
- Access to services should be logged and/or protected through access-control methods if possible.
- The most recent service packs, security patches and hot fixes must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use Admin when a non-privileged account will do.
- Servers and their input devices should be physically located in an access-controlled environment with all keys or locks set as per guidelines provided by systems management.
- Servers and workstations are specifically prohibited from operating from uncontrolled cubicle areas.
- Servers and workstations will be time synchronized across the entire network via active directory. The master timeserver will synchronize with an atomic clock. NTP will be used on all switches, Routers and Firewalls to synchronize time with the network. This will be restricted to the network administrator.
- All equipment with default manufacturer passwords will be changed to the Gatestone & Co. password policy standards.
- All systems will have Antivirus, DLP , external device control and internet control software installed.
- Recovery of critical systems will be within 4 hours with client information deemed critical.

## Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - All security related logs would be kept online for a minimum of 3 months
  - All security related logs to be kept offline on back up for 1 year.
  - Daily incremental tape backups will be retained for at least 1 month.
  - Weekly full tape backups of logs will be retained for at least 1 month.
  - Monthly full backups will be retained for a minimum of 2 years.
  - All backups will be kept in a secure limited access location.
- Security-related events will be reported to systems management, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host.
  - DLP events

### DLP prevention Events to monitor: Record the following events.

- Bank routing numbers with qualifying terms
- Credit or Debit Card numbers with Qualifying terms
- International bank account numbers
- US social Security numbers with qualifying terms.

Upon a finding investigate and determine if it's a breach and escalate to incident reporting team.

- It is the responsibility of the Systems Manager to review the audit logs produced by the iSeries and AS/400 operating system and to review the exception reports (detailing unauthorized access attempts) produced by PowerLock on a daily basis. Any anomalies are to be investigated and corrective action taken.
- Systems management will use any or all-available tools to monitor or scan for any vulnerabilities on the server.

## Compliance

- Audits will be performed on a regular basis by authorized organizations within Gatestone & Co.
- The internal audit group or systems management, in accordance with the Audit Policy, will manage audits.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

## Technical Compliance

The Technical Compliance team is responsible for the examination of operational and physical systems to ensure that hardware, software and physical security controls have correctly been configured and implemented.

They will review various procedures using the methods explained in the table below.

The testing team consists of:

Robert Coats: Security Officer  
 Edwin Saldhana: Facilities Coordinator

Vulnerability scans completed on our network will have findings recorded and mitigated in a timely manner.

The following table describes a schedule and list of evaluation factors for testing categories.

Category 1 systems are those sensitive systems that provide security for the organization or that hold SPI data from clients other critical functions. These systems include:

- + Firewalls, routers, and perimeter defense systems such as for intrusion detection,
- + Public access systems such as web and email servers
- + DNS and directory servers, and other internal systems that would likely be intruder targets.
- Database and files servers housing client SPI data.

Category 2 systems are generally all other systems, i.e., those systems that are protected by firewalls, etc., but that still must be tested periodically.

Test Type	Category 1 Frequency	Category 2 Frequency	Benefit
Network Scanning Nessus	Continuously to Quarterly	Monthly	<ul style="list-style-type: none"> <li>• Enumerates the network structure and determines the set of active hosts, and associated software</li> <li>• Identifies unauthorized hosts connected to a network</li> <li>• Identifies open ports</li> <li>• Identifies unauthorized services                             <ul style="list-style-type: none"> <li>• Identifies rogue wireless access points</li> </ul> </li> </ul>
Vulnerability Scanning Nessus	Quarterly or bi-monthly (more often for certain high risk systems), when the vulnerability database is updated	Monthly	<ul style="list-style-type: none"> <li>• Enumerates the network structure and determines the set of active hosts, and associated software</li> <li>• Identifies a target set of computers to focus vulnerability analysis</li> <li>• Identifies potential vulnerabilities on the target set</li> </ul>

			<ul style="list-style-type: none"> <li>Validates that operating systems and major applications are up to date with security patches and software versions</li> </ul>
Penetration Testing Third Party Metasploit	Annually	Annually	<ul style="list-style-type: none"> <li>Determines how vulnerable an organization's network is to penetration and the level of damage that can be incurred</li> <li>Tests IT staff's response to perceived security incidents and their knowledge of and implementation of the organization's security policy and system's security requirements</li> </ul>
Password Policy Review AD settings	Continuously to same frequency as expiration policy	Same frequency as expiration policy	<ul style="list-style-type: none"> <li>Verifies that the policy is effective in producing passwords that are more or less difficult to break</li> <li>Verifies that users select passwords that are compliant with the organization's security policy</li> </ul>
Log Reviews Event Tracker	Daily for critical systems, e.g., firewalls	Weekly	<ul style="list-style-type: none"> <li>Validates that the system is operating according to policies</li> </ul>
Virus Detectors Sophos	Weekly or as required	Weekly or as required	<ul style="list-style-type: none"> <li>Detects and deletes viruses before successful installation on the system</li> </ul>
Privilege access review	Quarterly	Annually	Review privilege user accounts to ensure only one or a few users to prevent data loss. This includes DBA, OS, Log server, Audit logs, AD, VPN, firewalls, backup and any other device holding or controlling SPI data
Review Encryption keys	Quarterly	Annually	Ensure keys are working and available and backed up to prevent data loss
Review development access and testing	Quarterly	Annually	Ensure testing and development are
IDS	weekly	Weekly	Ensure IDS and IPS are up to date and investigate any suspect compromises
File integrity Monitoring	Weekly	Weekly	Monitor critical files weekly and investigate.
Physical Security Review Card Access	Quarterly	Quarterly	<ul style="list-style-type: none"> <li>Repairs any vulnerabilities left by incorrectly following the terminated employee checklist.</li> </ul>
LAN Security Review Review AD Settings	Monthly	Monthly	<ul style="list-style-type: none"> <li>Removes access potentially left by incorrectly following the terminated employee checklist</li> </ul>



PCI Scanning	Quarterly on all External Web sites	Quarterly on all external web sites	<ul style="list-style-type: none"> <li>Part of the PCI compliance requirement</li> </ul>
Administrative account log review	Quarterly	Quarterly	<ul style="list-style-type: none"> <li>To ensure administrative accounts are secure and are not used for the proper purposes.</li> </ul>
Windows Update Review WSUS	Daily	Weekly	<ul style="list-style-type: none"> <li>Ensures that all PC's have had critical and non-critical patches installed in a timely manner.</li> </ul>
Application Testing	As Necessary	As Necessary	<ul style="list-style-type: none"> <li>Test all windows applications as necessary for security compliance using tools such as Nessus</li> </ul>
Wireless scanning	Bi annually	Daily	Review rogue systems daily for wireless functions also run specialized software to detect wireless hardware. Search with wireless adaptor and confirm each connection.

#### Hardening of Servers:

All servers will require a hardening before going live.

**Microsoft windows servers** - NSA guidelines will be followed in securing windows servers downloaded from their web site. The ports and services that are open will only include ports and services necessary for the server function only. All other services will be disabled. A list of approved ports and services will be created and approved by the change management committee and recorded as a baseline for that server.

List of auditing/configuration software to be used in conjunction is as follows

1. Microsoft baseline analyser
2. IIS lockdown tool
3. [SANS/FBI Top 20 List](#) (Most Critical Internet Security Vulnerabilities)
4. Nessus scan
5. Gatestone server install and hardening checklist

1

**LINUX Servers:** CERT guidelines will be followed in securing Linux/Unix servers. The ports and services that are open will only include ports and services necessary for the server function only. All other services will be disabled. A list of approved ports and services will be created and approved by the change management committee and recorded as a baseline for that server

List of auditing/configuration software to be used in conjunction is as follows

1. SE LINUX [Security-Enhanced Linux](#) (NSA)
2. [Apache](#) HTTP Server Security Tips (apache.org)
3. [SANS/FBI Top 20 List](#) (Most Critical Internet Security Vulnerabilities)
4. Nessus scan
5. Latest SAN threats

**Iseries:** IBM guidelines will be followed in securing Iseries server. The ports and services that are open will only include ports and services necessary for the server function only. All libraries and configuration items listed will be recorded while all other services will be disabled. A list of approved ports and services will be created and approved by the change management committee and recorded as a baseline for that server

List of auditing/configuration software to be used in conjunction is as follows

1. Nessus scans
2. [SANS/FBI Top 20 List](#) (Most Critical Internet Security Vulnerabilities)

### **Patch Management and End of Life software control:**

---

No software or hardware will be used after its end of life has expired.

Level 1: Critical patches will be applied to the OS in question within 1 week of release. An exception will be documented if this can't be accomplished.

Level 2: all other patches will be applied within 1 month of release.

- Patches will go through change management and testing before being approved. Patches will be tested before going live. As400 PFT's will be installed on the backup machine and installed live 15 days after they present no problems.
- Software or operating systems which are no longer supported by the vendor in question removed from operations at the earliest possibility. If the OS is part of a system that touches confidential information the system will be upgraded or removed immediately.

### **Patch management for Non-windows systems**

Non-windows systems will include firewalls, routers, switches, phone switches and Hardware components.

Critical security patch will be tested, approved by change management and applied within one week of discovery.

Non-critical patches will be tested and applied with approval of the change management team.

The administrator of each system has responsibilities to be aware of all patches and bring them to the change control rep for discussion. Refer to security practices of this document.

### **Remote User Access Control Policy**

---

This section describes aspects of our remote access procedures and all instances where an affiliate of Gatestone & Co. (staff or client) attempts to access Gatestone & Co. resources remotely. Remote

access implementations that are covered by this document include, but are not limited to the following:

- Citrix Web access/Internet

#### Remote Access - Two-Factor Authentication

Gatestone & Co. has accomplished this installing software on the Citrix server called Crypto. In order to satisfy the remote access needs for Gatestone & Co. and maintain a secure connection with two-factor authentication, the following strategy has been implemented:

The tokens for 2 factor authentication will be held in a secure server which will manage the lifecycle of the token.

Every user with remote access will be provided with a user ID, user ID code and a token which will present 8 characters minimum.

The token will produce Eight "Random" numbers which must be added to your user ID code in order to access Citrix.

When in Citrix the user must provide its user and password for the network.

Users will be locked out after 3 failed attempts.

#### Remote Access – Requests

- Gatestone & Co. units are responsible for requesting assistance with remote access implementations via helpdesk
- Security Officer will approve requests.
- All remote access is to be fully documented and stored.

#### Remote Access – Configuration and Control

- All computers connecting to Gatestone & Co. network via remote access will use anti-virus software with the most up-to-date definitions available.
- Remote access will be designed to prevent the storing of information on the local laptop. Exceptions will only be made if the client approves it in writing.
- All remote access machines will have an approved firewall installed and configured by Gatestone & Co. Presently Windows 10 professional are the approved firewalls.
- Only PC's, mobile devices and Laptops configured and locked down by Gatestone & Co. will be allowed connection privileges.
- Laptops will be whole disk encrypted with Bitlocker or disk locker.
- Mobile devices including smart phones will be encrypted.
- Locked down remote PC's will not allow any transfer of information. Print screens, Printers interfaces, CDROM, USB ports will all be disabled.
- Remote access users will be automatically disconnected from the Gatestone & Co.'s network after 30 minutes of inactivity. The user must then log in again to reconnect to the network. Pings or other artificial network processes are not to be used to keep a connection open. Exceptions to this rule must be reviewed and approved by Security Officer.

- The maximum connection time for a remote connection will be limited to 24 hours. Exceptions to this rule must be reviewed and approved by CSSD. Only one network connection is allowed.
- Information will not be downloaded to the remote site. Printers, and drive mapping are disabled on Citrix to prevent any files from being downloaded or uploaded from the remote site. Work is done locally and exclusively on Citrix only.
- All work is to be performed via the Citrix connection at 256bit encryption.
- Remote connections will be reviewed and compared to detect any connections not in use. Connections not used within 30 days will be deactivated.
- Remote connections to network equipment for administration will be encrypted.

#### Remote Access – Management and Monitoring

- Security Officer will grant permission and send an email to the operations department who will set up firewall and software control. Fill in form below and send to the Security officer.
- Security Officer will validate remote users every Quarter to determine continued need of each user and to verify correct access.

#### Remote Desktop support

- Remote support will require users to accept the invite for control. No invisible access and control is to be used.

#### Remote Access Checklist

Following the basic premise that unidentified sources and unidentified people will not be granted access, deciding the best method of granting access will be determined using the following guideline checklist:

Determine the database, system or application to be accessed:  
 Type of access requested: \_\_\_\_\_  
 Name of data resource(s): \_\_\_\_\_  
 Resource Sensitivity: \_\_\_\_\_  
 Owner of the resource: \_\_\_\_\_  
 IP Address: \_\_\_\_\_  
 Server Name: \_\_\_\_\_  
 List IP and Name of all servers: \_\_\_\_\_  
 Normal Access Procedure: \_\_\_\_\_  
 Access protocol: \_\_\_\_\_  
 Remote Location: \_\_\_\_\_  
 Business Reason for access: \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

Information Security will assist in determining type of access required in handling the business need:

When initiating a Pilot Project the installation of the protection on one or more servers will become a basis for planning the protection for the rest of the project resources. If any data on a server requires a

high level of protection due to its sensitive nature, the rest of the data on that device will be afforded the same high level of protection.

- Operations will log and review all remote access on a daily basis and look for anomalies. Anomalies will be escalated and investigated according to the Gatestone & Co. incident response program.
- Connections using Terminal Services, PC Anywhere, or any other remote access software are not permitted through firewalls; including DMZs. Exceptions to this rule must be reviewed and approved by Security Officer. These exceptions will be thoroughly documented.

#### Remote Access – Security Officer Responsibilities

- Development and maintenance of the Remote Access Guidelines and Procedures.
- Installation and maintenance of all equipment supporting Remote Access at Gatestone & Co.
- Performance and security monitoring for all steps of the Remote Access process.
- Responding to problems reported to the Technology Help Desk in accordance with standard procedures and levels of service.
- CSO reserves the right to refuse any request involving Remote Access that may compromise the security of the Gatestone & Co.'s networks.
- Validate Remote users' permissions Quarterly.

#### Remote Access – User Responsibilities

- Adherence to the CSSD Remote Access Guidelines, Procedures, Standards, and related guidelines and policies established by Gatestone & Co.
- It is the responsibility of the user to ensure that unauthorized users are not granted access to the Gatestone & Co. network through their remote connection.
- Implement the recommended security software, hardware settings, patches, and protocols on personal equipment used to access Gatestone & Co. network via remote access technology. Personal machines used in this manner become a de facto extension of Gatestone & Co. network.
- Follow all relevant Gatestone & Co. policies and procedures along with federal, state, and local laws pertaining to the security of sensitive and confidential data when working with such data on Gatestone & Co. networks.
- Immediately reporting known misuse or abuse of the network or associated equipment to the Technology Help Desk.
- Any person found to have violated this guideline would be subject to corrective action.
- Any lost or stolen Gatestone equipment will be reported to the help desk immediately.

#### Access and system monitoring Policy

Monitoring of IT resources for vulnerabilities on equipment will be conducted. This will be a daily check of relevant articles that will cover all physical and software resources used by Gatestone. Presently Gatestone uses

WatchGuard Firewalls: Subscription to Watchguard to keep abreast of latest security release  
Microsoft Windows 2012: Subscription to MS to keep abreast of vulnerabilities  
Allied Telesyn Switches and routers

Refer to the daily check list for a full list of resources used for this check.

This document will detail security controls and monitoring of user access for early identification of breaches or new vulnerabilities. Early ID of a breach will minimize potential impacts. Benefits included with these procedures include Compliance, Service Level Monitoring Limiting liability, Performance measuring and Capacity Planning.

Currently the subscriptions required are at minimum.  
Watchguard  
Sans institute daily email  
Microsoft security release

All monitoring logs will be compiled on a central server and monitored daily. These logs are to be kept for a minimum of 3 year.

#### PCI information

Monitoring: Daily and ongoing monitoring of logs are conducted by the operator 24/7 hours a day.

Events: Events and Escalation are co-related and presented to the CSO on a daily basis. Events and escalation are determined by the CSO at that time.

#### Client file access information

Monitoring: Daily and ongoing monitoring of logs are conducted by the operator 24/7 hours a day.

Events: Events and Escalation are co-related and presented to the CSO on a daily basis. Events and escalation are determined by the CSO at that time.

#### Antivirus Alerts

Monitoring: Daily and ongoing monitoring of logs are conducted by the operator 24/7 hours a day.

Events: Events and Escalation are co-related and presented to the CSO on a daily basis. Events and escalation are determined by the CSO at that time.

#### Internet Traffic:

Log storage: Firewall logs are stored on our central operations server via the event processor.

Monitoring: Daily and ongoing monitoring of logs are conducted by the operator 24/7 hours a day

Events: Events and Escalation are co-elated and presented to the CSO on a daily basis. Events and escalation are determined by the CSO at that time.

#### Mail:

Log storage: Mail and logs are stored and backed up on a daily basis via Tape.

Monitoring: Monitoring is only done on request basis.

#### Logon Information:

Log storage: User security logs are stored on the central operations server via Active directory. This will include remote access, IDS logs and any document auditing logs produced.

Monitoring: Once daily the logs are reviewed for anomalies. These include failed logon and locked user accounts.

## Firewall Build Policy

---

### Principles:

- Firewalls will be used to limit the interactions between networks
- The perimeter firewall system must control ALL traffic entering and leaving Gatestone & Co. internal network.
- The perimeter firewall system must provide a demilitarized zone (DMZ) capability where specified externally accessible services can be located
- Internal network segregation may use firewalls to deliver security zones or “trust levels”
- The firewall system must provide the capability to authenticate users before permitting access to resources protected by the systems
- All hardware components of the firewall must be located in a physically secure area

### Operation:

- Only firewall system administrators are permitted to logon to firewall hosts. The Security Officer can make exceptions.
- All changes to firewall access rules must be made through a single approved interface.
- Only personnel with the appropriate authorization can make changes to the firewall access rules, software, hardware or configuration.
- Logging and audit facilities provided by the firewall system must be fully utilized.
- The firewall system must be maintained to the highest standards.

### Configuration:

- The perimeter firewall system will be configured to deny any service unless it is expressly permitted
- The firewall Operating System will be configured for maximum security; i.e. hardened
- The firewall product suite must reside on dedicated hardware
- The initial build and configuration of the firewall must be fully documented
- There should be regular reviews to validate the firewall system meets the needs of the business regarding information security
- Security must not be compromised by the failure of any firewall component
- The firewall system will implement TCP/IP level filtering, and application level proxy mediation where appropriate.

### Firewall Detailed Configuration:

- VPN connections between offices and users will use SHA2 256/ HMAC with AES 256 encryption.
- Citrix connections will be NAT'd directly to the server using port 1494 only.
- FTP connections are only allowed IP to IP on a business need. Incoming FTP connections will be restricted to clients who need access to our server. All other FTP connections are restricted. This includes SSH on port 23 and regular FTP on port 21.
- SMTP will be forwarded to out DMZ antivirus/spam filter before being passed to our production server.



- No external connections to our firewalls will be allowed for configuration purposes
- ICMP pings will be blocked both incoming and outgoing by default. Testing pings allowed during testing only.
- Exe, avi, mp3, bat, pls, wmf, m3u extensions are blocked from entering through the firewall.
- Firewall configuration files will be backed up before and after any changes.
- HTTPS incoming connections are forwarded to Ccweb01 only.
- DNS queries on port 53 are allowed on outgoing connections only.
- Logging is enabled for all ports denied and allowed. This is recorded to the Event processor.
- DDOS protection will be enabled on the firewalls to protect from directed attacks.
- DMZ will be provided for all public facing servers that will pass through the firewall.

#### Firewall Change Control:

- Because they support critical Gatestone & Co. information systems activities, firewalls are considered to be production systems. This means that all changes to the software (Including vendor-provided upgrades and patches) must be approved in advance by the Information Security Manager, and then tested and approved by the Quality Assurance Department before being used in a production environment
- All firewall change requests have to complete a change request form (attached) and pass it to the Network Change Control Manger of the operations centre.
- Network control manager reviews and meets with the Information Security Manager for approval.
- Change control manager reviews the changes and communicates the changes and outcome to the initiator and all parties affected.
- The firewall configuration document is updated upon a successful change.
- Sample Change request form.

Refer to the appendix for definitions and help.

<b>CHANGE REQUEST #:</b>	<b>REQUEST DATE (DD/MM/YYYY):</b>
<b>Change Initiator:</b>	
<b>Contact phone:</b>	
<b>Change Implementer:</b>	
<b>Contact phone:</b>	
<b>Change Date:</b>	
<b>Change Time:</b>	
<b>Change Duration:</b>	
<b>System(s) Affected:</b>	

**DESCRIPTION OF CHANGE**

What?

Why?

References (change request # or Solve-IT Call#)

**IMPACT OF CHANGE**

Who will be affected by the change?

How will they be affected during the change?

How will they be affected after the change?

**SECURITY IMPACT OF CHANGE**

What is the risk of making the change and how is the risk being mitigated?

What is the risk of not making the change and how could that risk be mitigated?

What are the alternatives to the change?

**IMPLEMENTATION AND BACKOUT PLAN**

Implementation Plan:

Backout Plan:

TESTING OF CHANGE

Testing completed ok?

APPROVALS				
<i>Role</i>	<i>Name</i>	<i>Request approved signature</i>	<i>Request denied signature</i>	<i>Date</i>
Information Security Manager				

Request approved by

<p>Conditions on approval:</p>   	<p>Reasons for approval not given:</p>   
--	--

#### Contingency Planning:

- Technical staff working on firewalls must prepare and obtain Information Security Department approval for contingency plans which address the actions to be taken in the event of various problems including system compromise, system malfunction, and power outage.
- These contingency plans must be kept up-to-date to reflect changes in the Gatestone & Co. computing environment.
- These plans must also be periodically tested to ensure that they will be effective in restoring a secure and reliable computing environment.

#### Secure Back-Up:

- Current off-line back-up copies of firewall configuration files, connectivity permission files, firewall systems administration procedural documentation files, and related files must be kept close to the firewall at all times.
- A permissible alternative to off-line copies involves on-line encrypted versions of these files. Either of these options will help to keep trusted copies away from intruders, but at the same time immediately available to re-establish a secure and reliable computing environment.

#### Posting Updates:

- Because hackers and other intruders use the latest attack techniques, Gatestone & Co. firewalls must be running the latest software to repel these attacks.
- Where available from the vendor, all Gatestone & Co. firewalls must subscribe to software maintenance and software update services. Unless approved in advance by the Information Security Department Manager, staff members responsible for managing firewalls must install and run these updates within a week of receipt.

#### Monitoring Vulnerabilities:

- Gatestone & CO. staff members responsible for managing firewalls must subscribe the CERT (Computer Emergency Response Team) and Idefense© advisories and other relevant sources providing current information about firewall vulnerabilities.
- Any vulnerability which appears to affect Gatestone & Co. networks and systems must promptly be brought to the attention of the Information Security Department.

#### Audit and compliance

- Regular testing of the firewall will be carried out. Twice yearly an audit and testing of all firewall rules is to be carried out and approved by the Information Security Officer. The reviewer will look at all the rules and verify they are needed and are organized as securely as possible. This review will be recorded in the change control documents for the firewalls.
- There must be an active auditing/logging regime to permit analysis of firewall activity both during or after a security event

## **IDS (Intrusion Detection):**

---

### Log storage:

Watchguard logs are stored on a central database on ccsophos. The database is accessed on the central operations server via web browser.

### Monitoring:

Watchguard IPS/IDS logs are reviewed once per day. The list of anomalies are sorted and investigated. Events that are deemed serious are escalated to the CSO.

### Back up logs:

Log storage: Stored on "Backupserver2"

Monitoring: Backup logs are reviewed daily by the operator who reports all anomalies by 9am to the network administrator.

## Project Management and Change Management Controls

---

### Project Definition

A project is to be created on the projects database for absolutely every development work that needs to be done. This can go from a simple change to the development of a whole system. This includes all network components and databases.

### Projects Classification

There can be two kinds of projects:

**Formal requests:** These are projects related to any formal request from any department of the company. These kinds of projects require the approval of an AVP with the exception of Client Services, who can submit requests without an AVP's approval. The fact that a project has been approved by an AVP does not mean that the project will be activated. A cost and benefits analysis should be done to determine that the benefits are worth the costs. All formal projects will be prioritized and activated the weekly VP's meeting or via an urgent request from the requestor VP to the VP of Operations. Client Services Projects are exempted from the cost and benefits analysis requirements.

The cost and benefits analysis and project approval should be done as follows:

- The requestor must provide the benefits analysis of the project, which should indicate the monthly benefit represented in dollars and a detailed explanation of how will the project contribute to obtain such benefits.
- The developer must do the cost analysis and determine the cost of the project (please refer to the project costing document on the Appendix B).
- The developer should then, determine the return factor by applying the formula:  
$$\text{Monthly Benefits Amount} / \text{Cost Amount} * 100$$

This return factor represents the value or worthiness of the project and it should be considered when deciding what projects should get worked first. The higher the return factor is, the more resources the project should get.
- Once this costs and benefits analysis has been done it must be discussed with the requestor and it must be approved by the AVP.
- All projects with a cost higher than \$1000 must be approved by the Vice President of Operations.

**Problem fix/emergency projects:** These projects are related to any work needed to fix a problem or to attend an emergency. These projects do not require the approval of an AVP. It is to the Systems Development Manager's discretion to decide where or not a request should be treated as a problem or emergency project, or if it should be a formal request.

## Project Planning

Depending on the complexity of a project it may require the definition of a project plan. If so the project plan can be defined on the projects database or it can be done on a separate document, which should be attached to the project. See Appendix A for a suggested project plan model. This model is to be used as a reference, but a project may not contain all the phases defined in this model.

### Risk Assessment and Security Plan

A risk assessment and security plan must be done for all changes and projects. The project manager and the change control committee should do a thorough analysis to determine the severity of the changes or additions, risk factor and the levels of testing required for the project. The security plan addressing all security requirements such as data classification, user access, backup and recovery planning and business continuity will be defined and documented at this stage. The risk assessment will ultimately determine the security requirements and severity of the project.

<b>Risk Factor</b>	<b>Definition</b>
0	This represents a change or addition with virtually no risk, and would therefore require little quality assurance. An example of this would be a cosmetic change to a report or screen where no data is affected. Only unit testing would be required.
2	This factor will define a change or addition that affects a non-critical process or data. An example of this would be some calculation changes on a report or changes to a data file output for a client. Corrections to the change or addition would need to be done, but no recovery or recreation of data would be required. Unit testing, integration testing and user testing would be required.
4	This factor will define a change or addition that affects a mildly critical process or data and would require recovery in case of a failure. An example of this would be a process that updates or closes accounts for a single client on our system. A case like this would require corrections to the changes and recovery of data that may get corrupted. The levels of testing required would be: unit testing, integration testing, user testing and security testing.
6	This factor will define a change or addition that affects a highly critical process or affects critical or sensitive data. Some examples would be severe changes to the payroll system or changes to the nightly interest calculation process. These are changes that could cause a major stress to a client or to our own business. The levels of testing required would be: unit testing, integration testing, user testing, security testing and the definition of a recovery plan.
8	This risk factor would be used for major system enhancements that could bring the business to a halt if improperly implemented, such as an Intelec system upgrade or a change to a master file entailing a general system recompile. The levels of testing required would be: unit testing, integration testing, user testing, security testing, full system testing and the definition of a recovery plan.

### Testing and QA

A test plan is required for all projects. The plan must define how a project will be tested to the satisfaction of management and requestors. The different levels of testing will be determined based on the risk factor and severity of the project or change.



The plan will detail how a project will be tested: the level of testing required; who will be involved; when they will be involved; test cases required; security considerations, and any other pertinent information.

This plan should be reviewed by the appropriate levels of management including the Project Manager, the Requestor Manager and the Change Control Committee to ensure that nothing will be overlooked.

The ideal time to have the test plan and cases complete is at the time of the requirements submission to allow the developers to have further insight into what the requestor actually expects from the project.

### Testing levels

- **Unit testing:** this testing is to be done by the systems developer to prove that individual object changes work as expected.
- **Integration test:** this testing is to be done by the systems developer to prove that the integration between several objects or processes is correct.
- **User testing:** this testing will be done by the business analyst and/or requestor to ensure that all the expected business results are achieved.
- **Security testing:** this testing will be done by the change control committee to ensure that the changes or additions comply with our security standards such as encryption for file transfers; any new data to be stored is properly secured and accessible only to authorized employees, controls against common web vulnerabilities are in place, etc.
- **Full System testing:** this testing is to be done by system developers, business analysts, users and the change control committee to basically prove that all or most processes and operations will work correctly and will not be affected by a major change.

### Test Cases

Test cases are like experiments. They should include a purpose, the data required to test this purpose, the anticipated outcome along with the actual outcome.

In addition, a success or fail status will be given along with a reason for the failure. The failure could be for many reasons: program flaw, design flaw, requirements flaw, or for any other reason such as a hardware flaw, etc.

The results from all test cases must be documented, attached to the projects database and provided to the project manager for the approval of the implementation.

### Security Testing

Security testing must be done for all windows and web based programming. This security testing must include the following:

- Test cases for cross-site scripting vulnerability
- Test cases for SQL injection vulnerability

- Test cases for buffer overflow vulnerability
- Perform a Nessus vulnerability scan

#### Test Data

Test environment is created only based on client requirements. Test data is scrambled and scrubbed specifically for testing purposes so that no live data is used. Test data is immediately deleted upon completion of project requirement.

#### Back out plan

Backout plan is to be created and sent to the change control team for review with a timeline for when this will be implemented.

#### Post implementation testing

Final testing will get confirmation on whether all the project goals have been met.

#### Code Review

Once all the testing has been successfully completed the Systems Development Manager will move all the code involved to the implementation library and do a final review of the code to ensure that no faulty or malicious code may have been added. Once the review has been completed the Systems Development Manager must issue a report stating that the final code has been reviewed and that he approves it to be implemented.

#### Projects Approvals and Implementation:

The requestor, approver and implementer of a project must be by separate individuals to ensure the integrity of the change management system.

All projects must be approved by the project manager, the requestor manager and the change control committee, before they can be implemented and put into production.

**The Project Manager** must approve the implementation confirming that all the systems development tasks and tests were successfully completed and up to standards.

**The Requestor Manager or User** must approve the implementation confirming that the project meets the requirements to his/her satisfaction.

**The Change Control Committee** (of which the security officer is a member) must approve the implementation of the project confirming and ensuring that all security policies are being complied with and all risks to security and integrity of the data, network and facilities have been covered.

**Implementer** will wait for the approval from the requestor and the approval process before starting the implementation.

The approval must be in writing and it must clearly state that they approve the project to be implemented and promoted. This written approval will be attached to the projects database.

Once the project has been approved, the implementation will be done by the security administrator and the project manager. The Systems Development Manager responsible for the project will provide a list of sources and objects to be promoted. Implementation tasks may include but will not be limited to:

- Back up of old sources and objects - Security Administrator (SA)
- Promotion of new sources and objects - SA
- Data conversion - SA
- Installation of new software or hardware – Project Manager (PM) to request from Computer Operations
- User training sessions - PM
- Notification to users - PM

Once the implementation has been done, then a post-implementation review should take place. The project manager and the requestor manager should review and confirm that the change or addition is actually working as expected in the production environment.

Once the post-implementation revision has been done, then the project can be marked as completed on the projects database.

### Projects Database

Once a project is assigned to a developer, the developer is responsible for keeping the project updated on the projects database. The estimated completion date should be entered first. The status should be changed as the project moves to test. When the project is implemented, the status should be changed to complete and the development ending date and the approval date should be entered.

## Development and Programming

---

Developing will be hosted on a completely separate environment. No production data will be used for developing. If a program is to be promoted to the “live” environment the code will be reviewed and sent to the operations manager in charge of promotion.

### Tables

Developers are to use tables consisting of a physical file instead of hard coding codes or client numbers inside the programs, when more than 1 value may exist. For example, if a new business program will load accounts only for 1 client number it's fine to assign the client number inside the program. But if eventually the new business load is changed to load accounts to 2 client numbers, then a table should be created and the programs should be changed to obtain the numbers from the table.

## Modules

Developers are to approach a module-based style of programming; which is to always keep their eyes open for an opportunity of creating a module (a piece of code that could be re-used by other developers.)

This code should be extracted and converted into a module with parameters for it to be called.

## Intelec programs

- Under no circumstances should a developer copy a Quantrax program to any of the custom libraries (object or source).
- Developers are to avoid as much as possible to make modifications to Quantrax's programs. Only very minor changes that do not affect the program's logic can be done to programs inSCMOD only. These changes must be very well documented inside the program and an email must be sent to Quantrax providing full details of the changes made.
- Developers are to not include calls to custom programs from Quantrax's programs. Only the following Quantrax's programs should have calls to custom programs:
  - WACCUSCL in SCMOD (TAB menu)
  - ACLODPCLP1 in CCLIB (before new business posting)
  - ACLODPCLP2 in CCLIB (after new business posting)
  - PAYUPDCLP1 in CCLIB (before payment posting)
  - PAUUPDCLP2 in CCLIB (after payment posting)
  - CCNITLY1 in CCLIB (before nightly)
  - CCNITLY2 in CCLIB (after nightly)

## Library references

Developers are to not hardcode library references within RPG or CL programs. If needed, the object's library should be obtained by using the RTVOBJD command.

## Naming convention

- First 5 characters for an identification code, for Example:

CIBC	ALEGI (Alegis)	PAYRL (Payroll)
------	----------------	-----------------

- Next 2 characters for the object type, for Example:

RP (RPG)	PF (Physical File)	LF (Logical File)
CL (CL)	DF (Display File)	PR (Printer File)
DT (Data Area)		

- Next 2 characters for a sequence # from 1 to 99.

## Validations

Validate input and output. Whenever possible, validate all data being received, data being entered and data being exported. Generate exception reports to output any invalid values that may be found such as invalid dates, undefined codes, etc. Always validate codes against their tables respectively.

## Programming Languages

The following is the list of the programming languages allowed:

On the iSeries
RPGLE
RPGSQL: <i>limited to selections that will not generate a logical file</i>
JAVA: <i>limited for functions that cannot be perform with RPGLE</i>
CL
On PC programming
VB Script
JavaScript
HTML

**Note:** the use of any programming language not listed above is strictly prohibited.

## Generic Programming Standards

- Always compile programs using the highest warning level available for your compiler.
- Keep the design as simple and small as possible. Complex designs increase the likelihood that errors will be made in their implementation
- Deny access by default. Base access decisions on permission rather than exclusion. Access should be denied by default and the protection scheme should determine if access should be granted.
- Use comments to clarify - not echo - your code. Comments that merely repeat the code add to a program's bulk, but not to its value. In general, you should use comments for just three purposes:
  - To provide a brief program or procedure summary
  - To give a title to a subroutine, procedure, or other section of code
  - To explain a technique that isn't readily apparent by reading the source
- Always include a brief summary at the beginning of a program or procedure. This prologue should include the following information:
  - A program or procedure title
  - A brief description of the program's or procedure's purpose
  - A chronology of changes that includes the date, programmer name, and purpose of each change
    - A summary of indicator usage
    - Description of the procedure interface (the return value and parameters)
    - An example of how to call the procedure

## Programming Standards on the iSeries (RPG)

- New programs should not be written in RPG/400. All new programs are to be written with ILE RPG.

- The function keys used for online programming on the iSeries must follow the IBM standards: Enter=Enter, F1=Help, F3=Exit, F4=Prompt, F5=Refresh, F12=Cancel, F14=Print, etc.
- As we intend to head to a module based and object oriented environment (main benefits of ILE) developers should avoid writing programs with more than 1000 lines
- In order to ensure a structured programming environment, make programs easier to understand and to take advantage of the structured programming features that RPG ILE offers (procedures, functions, etc.). Developers should avoid the use of the instruction GOTO.
- Developers are to use existing modules and not create new programs to perform the same functions (i.e. FTP programs). As limitations are encountered on existing modules, developers must enhance them instead of creating duplicated ones.
- As developers see a particular logic or routine that could be re-used by other developers, they shall put this program in the REPOSITORY library. The program should be very well documented in order to make it easy to be reused.
- Declare all variables within D-specs. Except for key lists and parameter lists, don't declare variables in C-specs - not even using \*LIKE DEFN. Define key lists and parameter lists in the first C-specs of the program, before any executable calculations.
- Whenever a literal has a specific meaning, declare it as a named constant in the D-specs. This practice helps document your code and makes it easier to maintain. One obvious exception to this rule is the allowable use of 0 and 1 when they make perfect sense in the context of a statement. For example, if you're going to initialize an accumulator field or increment a counter, it's fine to use a hard-coded 0 or 1 in the source.
- Indent data item names to improve readability and document data structures. Unlike many other RPG entries, the name of a defined item need not be left-justified in the D-specs; take advantage of this feature to help document your code.
- Use indicators as sparingly as possible; go out of your way to eliminate them. In general, the only indicators present in a program should be resulting indicators for opcodes that absolutely require them (e.g., CHAIN before V4R2) or indicators used to communicate conditions such as display attributes to DDS-defined display files.
- Whenever possible, use built-in functions (BIFs) instead of indicators. As of V4R2, you can indicate file exception conditions with error- handling BIFs (e.g., %EOF, %ERROR, %FOUND) and an E operation extender to avoid using indicators.
- If you must use indicators, name them. V4R2 supports a Boolean data type (N) that serves the same purpose as an indicator. You can use the INDDS keyword with a display-file specification to associate a data structure with the indicators for a display or printer file; you can then assign meaningful names to the indicators.
- Use indicators only in close proximity to the point where your program sets their condition. For example, it's bad practice to have indicator 71 detect end- of-file in a READ operation and not reference \*IN71 until several pages later. If it's not possible to keep the related actions (setting and testing the indicator) together, move the indicator value to a meaningful variable instead.
- Don't use GOTO, CABxx, or COMP. Instead, substitute a structured alternative, such as nested IF statements, or status variables to skip code or to direct a program to a specific location. To compare two values, use the structured opcodes IF, ELSE, and ENDIF. To perform loops, use DO, DOU, and DOW with ENDDO. Never code your loops by comparing and branching with COMP (or even IF) and GOTO. Employ ITER to repeat a loop iteration, and use LEAVE for premature exits from loops.
- Don't use obsolete IFxx, DOUxx, DOWxx, or WHxxopcodes. The newer forms of these opcodes - IF, DOU, DOW, and WHEN - support free-format expressions, making those alternatives more readable. In general, if an opcode offers a free-format alternative, use it.

- Perform multipath comparisons with SELECT/WHEN/OTHER/ENDSL. Deeply nested IFxx/ELSE/ENDIF code blocks are hard to read and result in an unwieldy accumulation of ENDIFs at the end of the group. Don't use the obsolete CASxxopcode; instead, use the more versatile SELECT/WHEN/OTHER/ENDSL construction.
- Always qualify END opcodes. Use ENDIF, ENDDO, ENDSL, or ENDCS as applicable. This practice can be a great help in deciphering complex blocks of source.
- Use RPG IV's prototyping capabilities to define parameters and procedure interfaces. Prototypes (PR definitions) offer many advantages when you're passing data between modules and programs. For example, they avoid runtime errors by giving the compiler the ability to check the data type and number of parameters.
- Prototypes also let you code literals and expressions as parameters, declare parameter lists (even the \*ENTRY PLIST) in the D-specs, and pass parameters by value and by read-only reference, as well as by reference.
- Use a named constant to declare a string constant instead of storing it in an array or table. Declaring a string (such as a CL command string) as a named constant lets you refer to it directly instead of forcing you to refer to the string through its array name and index. Use a named constant to declare any value that you don't expect to change during program execution.
- Avoid using arrays and data structures to manipulate character strings and text. Use the new string manipulation opcodes and/or built-in functions instead.
- Use EVAL's free-format assignment expressions whenever possible for string manipulation. When used with character strings, EVAL is usually equivalent to a MOVE(P) opcode. Use MOVE and MOVE(P) only when you don't want the result to be padded with blanks.
- Avoid program-described files. Instead, use externally defined files whenever possible.

#### Standards for Windows and Web based Programming

- All web documents, whether static or generated programmatically, are to be written in accordance with web standards and must validate with the HTML Validator at the World Wide Web Consortium's web page (<http://w3c.org>). This will ensure consistency and maintainability of code, and also provide for standards compliant web pages that will render in any environment.
- All web documents must specify via DOCTYPE what version of HTML the document is written in to eliminate ambiguity and provide for the use of validation and testing tools.
- HTML documents are to contain structure only; all presentation will be specified using Cascading Style Sheets (CSS). This separation of structure and presentation will ease the task of maintenance and change control, and CSS elements can be reused by other developers to provide a consistent look and feel for all Gatestone & CO. web applications with minimal coding.
- Web documents and applications must be properly classified to ensure the content is appropriate for the audience. This classification will be used to ensure that access security to the web document or application can be properly applied in our Sharepoint environment.
- All web development should be done in a test environment. The PC of the developer needs to have a web server, database server, and the runtime environment of the development language configured and installed. This is to ensure that code will not affect the live environment and not affect operations.
- Programs, web pages, and anything else related to a web development project must remain on

the developer's PC until the project is approved for promotion. Testing can be performed by testers by using the IP address of the developer's machine.

- Software needs to be installed to synchronize the development environment on a developer's PC with an archive to cover for anything that should happen to the developer's PC.
- Code that is to be maintained must be installed onto the developer's PC so that it can be worked on outside of the live environment.
- Each perl program must "use strict" to ensure adherence to proper coding style for ease of maintenance.
- Each perl program must "use warnings" to highlight ambiguities and possible points of failure in the code. When run, the program must show no warnings.
- Each perl program that accepts input of any type from end users must "use taint" to ensure the security of Gatestone & CO.'s data, and also to enforce checks to avoid errant program behaviour resulting from unexpected user input. This mode prevents any data supplied by an end-user through any kind of input control to be unusable until it has been validated and verified to be accurate and correct. This ensures no Buffer Overflow attacks are possible. During the validation, any user input that is to be redisplayed within an HTML page to a browser must be cleaned of HTML entities to eliminate the possibility of Cross-Site Scripting attacks.
- Each perl program must make use of the facilities provided by the Carp module to facilitate tracing of program errors
- Any perl program that performs queries against a database must use the DBI (DataBase Interface) supplied with Perl, and use SQL with DBI's tokens. Statements must not be built directly from user input, since this allows for SQL Injection attacks.
- Perl code needs to conform to the suggestions in the Perl Style Guide, as distributed with Perl and also located at <http://www.perl.com/doc/manual/html/pod/perlstyle.html> -- Perl makes it very easy to write incomprehensible code, but by following correct style, code is easy to maintain.
- Wherever possible, program functionality needs to be encapsulated in a module that can be reused by other developers. Each module should be documented using Perl's POD system so that any developer using the module is clear on it's function and how it is used.
- Code will not be moved into production without a set of tests using Test::Harness that cover all aspects of the code's function as defined by the project originator. These tests need to be run anytime changes are made to the code to ensure the program operates as expected, as well as the tests for any other programs that could conceivably be affected by the promotion of the code being worked on. This testing will be done in accordance with Gatestone & CO.'s Change Control Policy.
- NEVER write code for which there is already an appropriate module; always search the Comprehensive Perl Archive Network (<http://cpan.org>) for a module that performs the function that needs to be coded to avoid reinventing the wheel. Any modules published under the Perl Artistic License (almost all of them) or released to the Public Domain are Freely Available and can be used for any purpose without obligation to the creator.
- Adhere to the principle of least privilege. Every process should execute with the least set of privileges necessary to complete the job. Any elevated permission should be held for a minimum time. This approach reduces the opportunities an attacker has to execute arbitrary code with elevated privileges.
- Sanitize data sent to other systems. Sanitize all data passed to complex subsystems such as command shells, relational databases, and commercial off-the-shelf (COTS) components. Attackers may be able to invoke unused functionality in these components through the use of SQL, command, or other injection attacks. This is not necessarily an input validation problem



because the complex subsystem being invoked does not understand the context in which the call is made. Because the calling process understands the context, it is responsible for sanitizing the data before invoking the subsystem.

- Use effective quality assurance techniques. Good quality assurance techniques can be effective in identifying and eliminating vulnerabilities. Penetration testing, fuzz testing, and source code audits should all be incorporated as part of an effective quality assurance program. Independent security reviews can lead to more secure systems. External reviewers bring an independent perspective; for example, in identifying and correcting invalid assumptions.

#### Promotion of code

The promotion of code will be done by the Security Administrator after the project has been approved as specified on the Projects Approvals and Implementation section of this document. The following is the basic procedure to be followed for the promotion of code:

- Backup existing sources in the backup source files:  
QCLSRC → QCLSRCBK  
QRPGSRC → QRPGSRC  
QRPGLESRC → QRPGLESRCB  
QDDSSRCS → QDDSSRCBK
- Copy the new sources from DEVLIB to the production library replacing the old sources (if they exist).
- Create the new files by using the CRTPF and CRTLF commands. If the files already exist, you must delete the old objects before you can create the new ones. Create a backup of the old files before you delete them if you need to copy the data to the new files.
- Compile the new sources for RPG's, DSPF's, PRTF's and CL's in the production library.

## Documentation

---

#### Standard user documentation

All user documentation should have a descriptive paragraph at the beginning. Explaining the purpose of the process, how it works and its frequency. Followed it should have the procedure. In some cases depending on the complexity of the process the documentation may have flowcharts, tables, diagrams and appendixes.

#### Standard system documentation

Developers are to add comments inside the programs explaining its purpose or changes done and also stating the date and name of the programmer who made the changes.

## Appendix A – Project Plan Model

---

1. Review and analyze problem and/or user specifications
2. Design preliminary product specifications
3. Review specifications with the user
4. Incorporate feedback to product specifications
5. Develop delivery timeline and budget
6. Analyze costs and benefits
7. Risk Assessment
8. Obtain approval to proceed
9. Develop detailed product specifications
10. Develop code
11. Developer's testing and debugging
12. Develop user's documentation
13. Develop user's testing specifications
14. Coordinate user's testing
15. Security Testing
16. Review testing results
17. Obtain approval for project implementation
18. Develop training specifications for end users
19. Coordinate user training sessions
20. Implement and promote into production

## Appendix B

---

### Preliminary Analysis and project cost calculation

- Time required for the discussion of the initial specifications. Consider the time on meetings for all the attendees and people involved in the project.
- Time for the analysis of the initial specifications and the calculation of the project cost.

### System Development

- Time for the Analysis & Project Planning
- Time for the Design
- Time for the Development
- Time for the Testing

### Documentation

- Time for the development of the documentation and procedures

### Training

- Time for the development of the training material
- Cost of training material.
- Time to perform the training. Considering the time of all the trainees.

### Capital Cost

- Purchase of Equipment
- Purchase of software

### Expenses

- Purchase of services
- Other Expenses. Consider expenses due to travelling, car rentals, food, etc.

Note: The time cost is to be calculated based on \$125 per hour per person for IT personnel and \$75 per hour per person for non-IT personnel

## Insider Threat Policy

---

Critical assets that Gatestone is tasked with protecting must have an insider threat component. Many reasons exist where insider threats are more dangerous. If the Security policy is applied to all users then this risk would be minimized.

1. Insiders know the network
2. Insiders know which data is most valuable
3. Insiders have legitimate user ID's

Insiders of high risk are considered the following. Privileged users, former employees, subcontractors and remote users. These users will be monitored closely for all access. Policy will apply to these users without exception.

The users above will have the following applied to them.

1. They are to have a unique user ID for all transactions
2. They are to have a daily user ID for main functions and a privileged user for administrative functions
3. All privileged users will be monitored with a daily log of activity generated and reviewed.
4. No security policy exception will be made for privileged user ID's.
5. Insider threat will be part of the onboarding training during security awareness.

During our annual risk assessment insider threat will be considered along with the requirements for our clients.

## Incident Response Policy

---

Systems covered: All systems that are considered critical to the good operation of Gatestone will be covered by this policy.

1. As400 and CRS systems
2. Phone switch and all components from dial tone to voice recordings
3. Network backbone including all exit and entry points
4. Email infrastructure
5. Backup systems

Analyzing the aftermath of a computer intrusion takes far longer than it takes a perpetrator to commit the crime. It is often the speed of the response that determines the outcome; and the more prepared an organization is when an incident first occurs, the quicker it can respond in the incident's wake. The protection of critical IT resources requires not only adopting reasonable precautions for securing these systems and networks, but also the ability to respond quickly and efficiently when system and network security defences have been breached.

Unfortunately, responding to computer security incidents is generally not an easy endeavour. Proper incident response requires technical knowledge, communication, and coordination among personnel in charge of the response process.

In information technology, incident refers to an adverse event in an information system and/or network or the threat of the occurrence of such an event. Examples of incidents include unauthorized use of another user's account, unauthorized use of system privileges, and execution of malicious code that destroys data. Other adverse events include floods, fires, electrical outages, or excessive heat that results in system crashes. Adverse events such as natural disasters and power-related disruptions, though certainly undesirable incidents, are not generally within the scope of incident response teams and are better addressed by Gatestone & CO.'s business continuity plans. For the purpose of incident response, therefore, the term incident refers to an adverse event that is related to information security.

- Gatestone & CO. will provide yearly tests and training for those responsible for the incident handling.

### Types of Incidents

The term incident encompasses the following general categories of adverse events:

*Malicious code attacks.* Malicious code attacks include attacks by programs such as viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is typically written in such a manner that it masquerades its presence, making it difficult to detect. Furthermore, self-replicating malicious code such as viruses and worms can replicate rapidly, thereby making containment especially challenging.

*Unauthorized access.* Unauthorized access encompasses a range of incidents from improperly logging into a user's account (for example, when a hacker logs in to a legitimate user's account) to unauthorized access to files and directories stored on a system or storage media by obtaining super-user privileges. Unauthorized access may also entail accessing network data by planting an unauthorized sniffer program or device to capture all packets traversing the network at a particular point. This also includes planting a wireless device on Gatestone's network that is not authorized.

*Unauthorized utilization of services.* It is not absolutely necessary to access another user's account to perpetrate an attack on the system or network. An intruder may also obtain access to information or plant Trojan horse programs by misusing available services. Examples include using the network file system (NFS) to mount the file system of a remote server machine or inter-domain access mechanisms in Windows NT to access files and directories in another organization's domain.

*Disruption of service.* Users rely on services provided by network and computing services. Those with malicious intent can disrupt these services in a variety of ways, including erasing critical programs, mail spamming (flooding a user account with electronic mail), and altering system functionality by installing Trojan horse programs.

*Misuse.* Misuse occurs when someone uses a computing system for other than official purposes, such as when a legitimate user uses a Gatestone & CO. computer to store personal records.

*Espionage.* Espionage is stealing information to subvert the interests of a corporation or government.

*Hoaxes.* Hoaxes occur when false information about incidents or vulnerabilities is spread.

*Misconfiguration.* Configuration errors on software and hardware which impacts security.

#### Automated systems for support with Incident handling.

- IDS system Sophos
- Sophos logs for Virus detection and implementation
- Firewall WatchGuard logs to detect unauthorized attacks
- Event viewer used to detect unauthorized
- Journal logs from the Iseries

#### Legal and SLA Incident Reporting Requirements

All incidents must be reported according to the Incident Response Procedure. However, incidents involving the theft or loss of personal consumer information **must** be reported to the client no more than 24 hours subsequent to the incident's discovery . The calling tree for the client will be used and kept up to date. This will include any regulatory, government, enforcement investigation or private

proceeding related to your data handling practices. This is to comply with certain US state and federal laws with regards to identity theft and financial institutions. User can call the help desk for further clarification of incident reporting.

Note: Employees will assist vendors, clients, federal and provincial authorities with their incident control program investigations.

BOA special considerations: Please see Bank of America incident response procedure.

#### Incident Reporting outside Gatestone & Co.

All incidents that contravene state, provincial or federal laws will be escalated to the responsible executive. The Executive team will decide to call the appropriate authorities at that time and inform the Chief Security Officer of the situation.

All emergency situations will be escalated to highest-level possible using Gatestone & CO.'s incident report team below. The incidence response member will contact the appropriate service and make contact with executives and Chief security Officer.

User can call the help desk for further clarification of incident reporting.

#### Incident Response Roles and Responsibilities

##### Executives

The executive team is responsible for ensuring a representative attends all meetings regarding minor Incidents. They are also to be informed of all major incidents immediately, in order to take necessary ownership and offer direction during the incident resolution.

##### Users

It is the responsibility of any user, of technical background or not, from base employee to executive, to report any suspected security incident to the Help Desk.

##### Help Desk

The Help Desk analyzes the incident, and determines its level of severity based on its impact. Assuming the incident is legitimate, the incident will be dealt with accordingly. They will also assist the Security Officer, Systems Administrator, and Network Administrator as necessary.

##### Security Officer

Will thoroughly investigate all major incidents, and perform the necessary preventative steps to isolate the incident so it can be dealt with by the necessary entities. They will also ensure that all parties who need to be involved have been contacted. Training of Security officer will include CISSOP or similar training to cover all security breach responsibilities.

Responsible for changes to this plan to adopt to changes in the industry and best practices. This will also include lessons learned in following similar incidents.

#### Systems Administrator

Responsible for dealing with systems-level incidents, performing necessary steps for eradication of reported incidents and necessary steps to prevent future incidents as possible.

#### Network Administrator

Responsible for dealing with network-level incidents, performing necessary steps for eradication of reported incidents and necessary steps to prevent future incidents as possible.

#### Incident Response Team

The incident response team has been assembled from technical staff within our IT department. They will oversee the response to all reported incidents, as well as assessing incidents and vulnerability reports to determine the best possible way to protect our systems and assets. The team is to meet weekly to review incidents or more frequently as circumstance dictates. The executive team will always have a representative in the Incident Response Team.

#### Team members

Nicholas Wilson	Chairman and C.E.O.
John Tilley	President
Nicholas Dowd	Executive Vice President and C.F.O.
Claude LaPointe	IT director
Robert Coats	Information Security Officer
Ali Khan	Manager, Computer Operations

Please refer to the Corporate Intranet for contact information.

#### Evidence Handling

Investigating and handling of evidence will follow the policy below to ensure a fair and neutral stance by Gatestone & Co.

#### Clear chain of custody:



- All evidence will be collected and held by a neutral party.
- Evidence will be held by Human resources in a locked and tamper proof cabinet.
- A Clear chain of custody will prevail for all evidence. This means that Gatestone & CO. must guarantee that no non-neutral party has had access to said evidence.
- A sign off and statement by the evidence collector will be required when evidence is presented to Human resources. This will be kept with the evidence in question
- A sign off will be required for anyone looking at the evidence and details on how the information is gathered. IE. Laptop investigation.

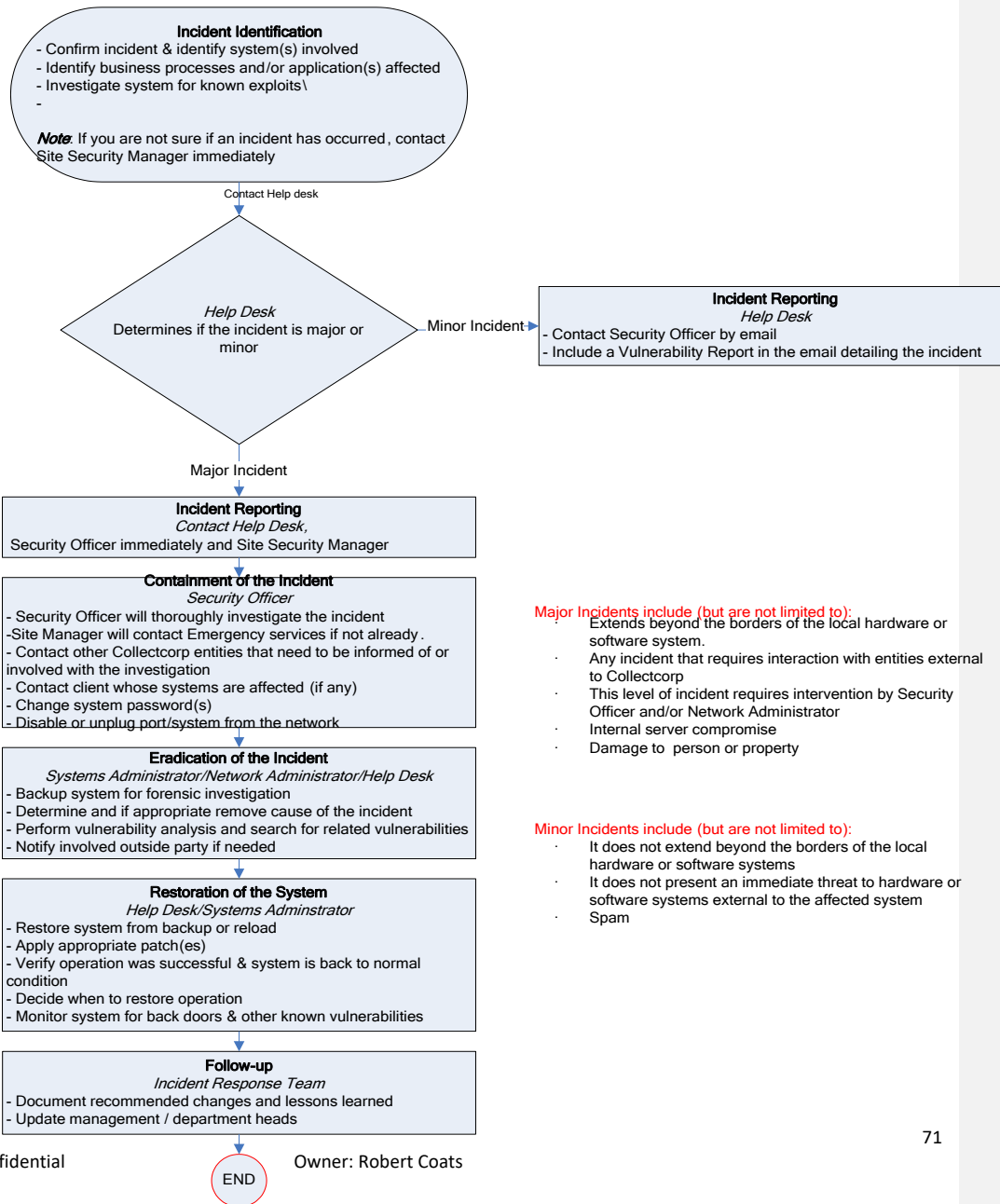
Weight of Evidence: All evidence will be collected in an impartial manner.

- All Evidence will be collected during each incident and separated from all others information. This means Logs, laptops, email, will be copied saved and stored following the chain of Custody.
- Gathering of Evidence will follow all privacy laws.
- Based on chain of custody and privacy laws admissibility will be established by the CSO

Evidence gathering: Photographs, Logs, Hardware (laptops, PDA's ect)

- The date the item was collected will be clearly labeled as such.
- Statement by the investigator regarding the circumstances of the evidence, including a clear description on how the chain of custody was maintained.

# Incident Response Procedure



**Major Incidents include (but are not limited to):**

- Extends beyond the borders of the local hardware or software system.
- Any incident that requires interaction with entities external to Collectcorp
- This level of incident requires intervention by Security Officer and/or Network Administrator
- Internal server compromise
- Damage to person or property

**Minor Incidents include (but are not limited to):**

- It does not extend beyond the borders of the local hardware or software systems
- It does not present an immediate threat to hardware or software systems external to the affected system
- Spam

## E-mail Internet and acceptable use Policy

1. The following policy with regard to the use of Gatestone & CO.'s E-mail and Internet systems has been in place since May 8, 2000. The purpose of this policy is to protect Gatestone & CO. Inc., its employees and clients from loss or embarrassment, as well as to ensure that all facilities are used appropriately.
2. The Internet and E-mail systems in use at Gatestone & CO. are business tools and must not be used for non-business purposes. Non-business purposes include the display and distribution of games, jokes, pornographic material and personal e-mails. The use of instant messaging, is not permitted, unless the software has been approved by the Corporate Security Officer and Senior management.
3. The use of Hotmail, MSN mail, Yahoo and other external email accounts are prohibited. Incoming emails from these services have been blocked by our system due to security concerns.
4. E-mail users will be restricted to sending e-mails to other Gatestone & CO. users (e-mail users with an @Gatestone & CO..com address). The Vice President of each division must authorize, in writing, users who are able to send and receive e-mails outside Gatestone & CO..
5. Employees must not use the e-mail system for sending letters to debtors that have not been approved by the client and by Quality Assurance. This could expose Gatestone & CO. to the possibility of losing a client or suffering financial loss or legal penalties.
6. Should an employee change departments, they must be re-qualified for e-mail and Internet use.
7. There will be a periodic review of any individual's mailbox to see if content adheres to company policy.
8. Automated tools will be put into place that will consistently monitor use of the Internet and E-mail systems. Inappropriate use will be reported to senior management and access privileges will be withdrawn immediately. Only the President can authorize exceptions to this policy.
9. The size limit on files that can be transferred will be 1 MG. The maximum allotment of space for each user is 40 MEG. Exceptions can be made for specific users who routinely transmit or receive large volumes of data for business purposes.
10. Junk mail must not be forwarded. This is a waste of time, space on the system and valuable resources. The most common form of junk mail is an e-mail advising you to forward the e-mail to as many users as you can. This is used by the originator to collect user ID's through the e-mail system. The person originating the e-mail can gather the names, as well as e-mail addresses, and send junk mail out to this collected list of users. Junk mail often includes such things as free offers, equipment, phones, etc.
11. Signatures should be used on all e-mails to properly identify the sender and should include name, title and phone number.

- Internet file sharing programs (KAZZA, NAPSTER, etc) as well as connection to radio stations and permanent information services (ticker tape, news, etc.) that could affect our communications bandwidth are prohibited.

## Separation/ Segregation of Duties

---

### Explanation

A control procedure whereby the active involvement of two people is required to complete a specified process. Such control may be physical; e.g. two persons required unlocking the Data Safe, or logical; as in the case of a higher level authorisation password required to permit the entry of data created or amended by another person.

Dual Control is one of the foundations of Information Security as it is based upon the premise that, for a breach to be committed, then both parties would need to be in collusion and, because one should always alternate the pairs of people, it would require a much greater level of corruption in order to breach dual control procedures; especially is such procedures require nested dual control access, such that (say) 2 pairs of people are required to enable access.

See Roles and Responsibilities policy below

### Procedure

- All security-related changes must be performed separately from the person who authorizes the change. (User creation, granting authority, etc).
- All security-related changes must be documented and reviewed monthly, detailing who requested the change, and who.

\_\_\_\_\_

Name

\_\_\_\_\_

Signature

Acknowledgement

\_\_\_\_\_

Human Resources

## Roles and Responsibilities

---

In addition to the specific roles outlined below, it is the responsibility of every user to ensure the integrity of sensitive information is maintained by:

- Following existing security policies regarding sensitive information
- Maintaining a clean desk
- Disposing of all sensitive information by shredding
- Discretion and compliance with any and all NDA's applicable
- Ensuring the integrity of all data under their ownership
- Being aware of and complying with Gatestone & CO. policies and procedures

### Executives

- Review and approve/deny any policy changes
- Review and approve/deny any permission changes for staff reporting to them
- Kept informed of all critical-level incidents and steps taken for resolution
- Inform IT/HR of any role changes for their manager-level staff
- Executives must be represented in all aspects of Risk Management, including the Change Control Committee, and Incident Response Teams
- Ensure, through policies and procedures that all applicable laws, contractual obligations, and regulatory regulations are adhered to.

#### **CEO**

- Accountable for the overall risk of the company
- Delegates day to day operational and IT responsibilities to other executives.
- Ensures that all aspects of the organization are following best practices for Information Security.

#### **President**

- Reports major risk issues to CEO.

#### **CFO**

- Accountable for the funding and definition of business needs.
- Works with IT to ensure Information Security plans are in place.

#### **CTO**

- Accountable for Information Technology risk management.
- Responsible for implementing and ensuring the Information Security program is in place and follows industry best practices.
- Reports security issues and needs to CEO.

#### **Director of HR**

- Accountable for the security of all business personnel
- Reports issues to CTO as necessary
- Responsible for ensuring HR staff follows information security best practices

## Business Personnel

- Senior business personnel are accountable for managing information assets related to their area (Information Owners). The Information Owners will:
  - Approve business use of information
  - Determine security classification of each segment of data
  - Define departmental access roles and assign access for individuals based on their need to know
  - Ensure that all department/unit personnel with access to information assets are trained in relevant security and confidentiality policies and procedures
- Business personnel are also fully responsible and accountable for ensuring day-to-day compliance with all Information Security best practices
- Ensure implementation and of policies, and, documentation of process and procedures for guaranteeing availability of systems, including:
  - Risk assessment
  - Data backup plan
  - Disaster recovery
  - Emergency mode operation
  - Software testing and revision controls

### ***Managers***

- Inform IT/HR of role changes for their staff
- Ensure staff under care follow all security policy and procedures
- Changes to policy are to be communicated and enforced to all staff.
- LAN access to shared manager's folder, as well as a personal storage allocation
- Controlled LAN access to client-related data based on scope of responsibility
- Able to email both externally and internally through corporate Exchange server
- Able to reset user IDs on iSeries (not domain) for business Supervisors and below

### ***Supervisors***

- Inform IT/HR of role changes for their staff
- LAN access to shared supervisor's folder, as well as a personal storage allocation
- Controlled LAN access to client-related data based on scope of responsibility
- Able to email both externally and internally through corporate Exchange server
- Able to reset user IDs on iSeries (not domain) for business users

### ***Users***

- Limited LAN access for domain access only
- Restricted access to data based on the business client they are assigned to
- Seek access to data only through the authorization and access control process.
- Access only that data which s/he has a need to know to carry out job responsibilities.
- Disseminate data to others only when authorized.
- Report access privileges inappropriate to job duties to the Information Owner for correction.
- Attend training in security and confidentiality policies/procedures.
- Attest in writing to knowledge of and compliance with health-related security and confidentiality policies and procedures prior to accessing protected health information.

## Support Personnel (non-IT)

### ***Human Resources***

- Access to employee records
- Access to shared Human Resources network folder, as well as a personal storage allocation
- Able to email both externally and internally through corporate Exchange server
- Maintain current status of all employee roles and physical (building) security access
- Submit new hire/termination report to IT for the purpose of disabling or adding users
- Able to email both externally and internally

### ***Client Services***

- LAN access to shared customer service folder, as well as a personal storage allocation
- LAN access to dedicated client folders, per the scope of their position (reps are dedicated to certain clients)
- Able to email both externally and internally

### ***Accounting***

- LAN access to shared customer services folder
- Access to ACCPAC accounting software
- Access to payroll information
- Responsible for authorising and processing payments from consumers

### ***Compliance***

- LAN access to folders containing Policies and Employee Recordings for review
- Responsible for authorising and processing payments from consumers
- Responsible for ensuring all staff are trained and licensed as necessary based on their job function
- Review staff periodically for legal compliance as well as compliance with company policies

## Information & Technology

### ***Systems Development Manager***

- Responsible for reviewing development projects and assigning priority based on the project's impact
- Risk and impact assessment of new projects and updates to any development tools before implementing
- Verify test results and promote completed code
- Access to development environment
- Read-only access to live environment
- LAN access to folders with development tools and file transfer folders
- Access to personal storage folder on LAN
- Able to email both externally and internally

### ***Programmer/Analyst***

- Responsible developing and testing new code slated for production
- Access to development environment only
- LAN access to folders with development tools and file transfer folders
- Access to personal storage folder on LAN

- Able to email both externally and internally

#### ***Computer Operations Manager***

- Review new user IDs created by HR
- Critically analyze any permission change request to ensure they follow policy
- Risk and impact assessment of any systems upgrade or change
- Ensure that Computer Operations functions comply with policies
- To be informed of and provide direction for any major incident
- Able to email both externally and internally

#### ***Computer Operations Supervisor***

- Assist and inform Computer Operations Manager of any incidents and their status
- Respond to incidents escalated by Computer Operations/Helpdesk
- Assign/revoke permissions on LAN and MS Exchange server
- Ensure Help Desk complies with policies
- Ensure SLA levels are being met
- Able to email both externally and internally

#### ***Computer Operations***

- Perform nightly operations duties
- Monitor nightly process
- Monitor system backup
- Escalate minor incidents to Help Desk
- Escalate major incidents to Computer Operations Supervisor/Manager
- Limited read-only LAN access to ensure processes are running correctly

#### ***Help Desk Technician***

- Provide desktop support
- Ensure SLA levels are met for desktop operation
- Monitor system status
- Escalate major incidents to appropriate group(s) as necessary according to Incident Response policy
- Change LAN security permissions on approval
- Reset user passwords
- Able to email both externally and internally

#### ***Network Administrator***

- Risk and impact assessment of any network changes
- Develop and maintain network infrastructure and performance
- Build and maintain critical network components and security
- Respond to escalated incident reports
- Administrative access to LAN / Network components
- Assess network/firewall change requests and approve/deny according to policy
- Ensure change requests are implemented according to policies
- Able to email both externally and internally



**Network Technician**

- Monitor network activity for incidents and escalate according to Incident Response policy
- Monitor firewall logs for incidents and escalate according to Incident Response policy
- Implement network/firewall change requests which have been approved
- Administrative access to LAN / Network components
- Escalate major incidents according to Incident Response policy
- Able to email both externally and internally

**Security Administrator/Privacy Officer**

- Access to firewall / network logs
- Assess security change requests and approve/deny according to policy
- Monitor firewall change logs to ensure changes comply with policy
- Respond to escalated incident reports
- Able to email both externally and internally
- Ensure compliance with privacy policy's including web page privacy policy
- Make sure security policy's align with legal requirements.
- Assist Business Owners in assessing their data for classification and advise them of available controls

**Sign off**

---

This document and corresponding recommendations have been reviewed and accepted by the parties below.

**I.T. Department**

Dated this \_\_\_\_\_ day of \_\_\_\_\_, in the year \_\_\_\_\_.

\_\_\_\_\_  
Claude LaPointe  
IT director

## Appendix A – Basic Security Concepts

---

### Confidentiality

When information is read or copied by someone not authorized to do so, the result is known as *loss of confidentiality*. For some types of information, confidentiality is a very important attribute. Examples include research data, medical and insurance records, new product specifications, and corporate investment strategies. In some locations, there may be a legal obligation to protect the privacy of individuals. This is particularly true for banks and loan companies; debt collectors; businesses that extend credit to their customers or issue credit cards; hospitals, doctors' offices, and medical testing laboratories; individuals or agencies that offer services such as psychological counselling or drug treatment; and agencies that collect taxes.

### Integrity

Information can be corrupted when it is available on an insecure network. When information is modified in unexpected ways, the result is known as *loss of integrity*. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting.

### Availability

Information can be erased or become inaccessible, resulting in *loss of availability*. This means that people who are authorized to get information cannot get what they need.

Availability is often the most important attribute in service-oriented businesses that depend on information (e.g., airline schedules and online inventory systems). Availability of the network itself is important to anyone whose business or education relies on a network connection. When a user cannot get access to the network or specific services provided on the network, they experience a *denial of service*.

### Authentication, Authorization, and Non-Repudiation

To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. *Authentication* is proving that a user is whom he or she claims to be. That proof may involve something the user knows (such as a password), something the user has (such as a "smartcard"), or something about the user that proves the person's identity (such as a fingerprint). *Authorization* is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program.

Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted - the user cannot later deny that he or she performed the activity. This is known as *non-repudiation*.

## Privacy

---

It is the policy of Gatestone & Co. to operate and observe privacy guidelines as set out in the PIPEDA, PIPA and legislation (CANADA) as well as GLBA safeguards rules in the United States. It is the commitment of Gatestone & Co. to protect the privacy interests of its clients and the customers of those clients.

Privacy awareness training will be conducted for privacy regulation and policy at at time of hire and annually after that.

Rules, guidelines and safeguards have been implemented to protect personal information against loss, or theft as well as to prevent unauthorized access, disclosure, copying, use or modification of such information. Our procedures also address the retention and destruction of this information. This is achieved through, but not limited to, shredding services, encryption, clean desk policy, privacy education seminars, confidentiality agreements, a security system based on access levels, masked windows, enhancements in programming and the appointment of a Gatestone & CO. Privacy Ombudsman.

These rules, guidelines and safeguards will be continuously reviewed in order to adapt as privacy legislation is amended and/or created.

## Clean Desk Policy

---

It is Gatestone & CO. policy that all Gatestone & CO. employees adhere to a Clean Desk Policy.

The purpose of the policy is to help ensure all client data is not at risk of being exposed to anyone who should not have access to it. A clean desk policy helps prevent information from being taken and or read by people such as cleaning staff, contractors, janitorial staff, building employees, visitors or anyone else who might have access to our facility.

When you are not at your desk, it should be clear of any work related documentation. All Documents are to be stored in a lockable drawer or filing cabinet.

Periodic and unannounced inspections will be performed to ensure adherence to this policy. Any employee who fails to comply with this policy will be subject to disciplinary action, which may include dismissal.

## PCI compliance Policy

---

- Track data (cards magnetic strip) is not stored under any circumstances
- 3 Digit or 4 digit card verification codes or values printed on the front of the card (CVV2, CVC2 and CAV2 data) are not stored under any circumstances.

- PIN numbers or identification numbers are not stored under any circumstances.
- Card holder data that is stored or transmitted is to be encrypted. Please see encryption policy detailing allowed encryption protocols.
- Card holder data will be limited to the individuals whose job requires it only and no one else.
- Where Card holder data is used on our web site a Quarterly scan of that PC will be done by an approved scanning vendor qualified by PCI SSC.
- A yearly external and internal penetration scan will be done on Gatestone's network or when a major change has occurred on the network. This will include network and application layer scanning.
- Live CC numbers will not be used for the testing environment.

## Appendix B – Types of Security Incidents

---

### Probe

A probe is characterized by unusual attempts to gain access to a system or to discover information about the system. One example is an attempt to log in to an unused account. Probing is the electronic equivalent of testing doorknobs to find an unlocked door for easy entry. Probes are sometimes followed by a more serious security event, but they are often the result of curiosity or confusion.

### Scan

A scan is simply a large number of probes done using an automated tool. Scans can sometimes be the result of a misconfiguration or other error, but they are often a prelude to a more directed attack on systems that the intruder has found to be vulnerable.

### Account Compromise

An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges (privileges a system administrator or network manager has). An account compromise might expose the victim to serious data loss, data theft, or theft of services. The lack of root-level access means that the damage can usually be contained, but a user-level account is often an entry point for greater access to the system.

### Root Compromise

A root compromise is similar to an account compromise, except that the account that has been compromised has special privileges on the system. The term root is derived from an account on UNIX systems that typically has unlimited, or "super user", privileges. Intruders who succeed in a root

compromise can do just about anything on the victim's system, including run their own programs, change how the system works, and hide traces of their intrusion.

#### Packet Sniffer

A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require privileged access. For most multi-user systems, however, the presence of a packet sniffer implies there has been a root compromise.

#### Denial of Service

The goal of denial-of-service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial-of-service attack can come in many forms. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data.

#### Exploitation of Trust

Computers on networks often have trust relationships with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.

#### Malicious Code

Malicious code is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malicious code includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self-replicating programs that spread with no human intervention after they are started. Viruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial of service, and other types of security incidents.

#### Internet Infrastructure Attacks

These rare but serious attacks involve key components of the Internet infrastructure rather than specific systems on the Internet. Examples are network name servers, network access providers, and large archive sites on which many users depend. Widespread automated attacks can also threaten the infrastructure. Infrastructure attacks affect a large portion of the Internet and can seriously hinder the day-to-day operation of many sites.

## Appendix C - Anatomy of a Security Policy

---

### Security Policies

A security policy is a documented high-level plan for organization-wide computer and information security. It provides a framework for making specific decisions, such as which defence mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long-term document, the contents should avoid technology-specific issues.

A security policy covers the following (among other topics appropriate to the organization):

- High-level description of the technical environment of the site, the legal environment (governing laws), the authority of the policy, and the basic philosophy to be used when interpreting the policy
- Risk analysis that identifies the site's assets, the threats that exist against those assets, and the costs of asset loss
- Guidelines for system administrators on how to manage systems
- Definition of acceptable use for users
- Guidelines for reacting to a site compromise (e.g., how to deal with the media and law enforcement, and whether to trace the intruder or shutdown and rebuild the system)

A *network security incident* is any network-related activity with negative security implications. This usually means that the activity violates an explicit or implicit security policy

Factors that contribute to the success of a security policy include management commitment, technological support for enforcing the policy, effective dissemination of the policy, and the security awareness of all users. Management assigns responsibility for security, provides training for security personnel, and allocates funds to security. Technological support for the security policy moves some responsibility for enforcement from individuals to technology. The result is an automatic and consistent enforcement of policies, such as those for access and authentication. Technical options that support policy include (but are not limited to)

- Challenge/response systems for authentication
- Auditing systems for accountability and event reconstruction
- Encryption systems for the confidential storage and transmission of data
- Network tools such as firewalls and proxy servers

### Security-Related Procedures

Procedures are specific steps to follow that are based on the computer security policy. Procedures address such topics as retrieving programs from the network, connecting to the site's system from home or while travelling, using encryption, authentication for issuing accounts, configuration, and monitoring.

### Security Practices

System administration practices play a key role in network security. Checklists and general advice on good security practices are readily available. Below are examples of commonly recommended practices:

- Ensure all accounts have a password and that the passwords are difficult to guess. A one-time password system is preferable.
- Use tools such as MD5 checksums (8), a strong cryptographic technique, to ensure the integrity of system software on a regular basis.
- Use security programming techniques when writing software. These can be found at security-related sites on the World Wide Web.
- Be vigilant in network use and configuration, making changes as vulnerabilities become known.
- Regularly check with vendors for the latest available fixes and keep systems current with upgrades and patches.
- Regularly check on-line security archives, such as those maintained by incident response teams, for security alerts and technical advice.
- Audit systems and networks, and regularly check logs. Many sites that suffer computer security incidents report that insufficient audit data is collected, so detecting and tracing an intrusion is difficult.

#### Intrusion Detection

Research is underway to improve the ability of networked systems and their managers to determine that they are, or have been, under attack. Intrusion detection is recognized as a problematic area of research that is still in its infancy. There are two major areas of research in intrusion detection: anomaly detection and pattern recognition.

Research in anomaly detection is based on determining patterns of "normal" behaviour for networks, hosts, and users and then detecting behaviour that is significantly different (anomalous). Patterns of normal behaviour are frequently determined through data collection over a period of time sufficient to obtain a good sample of the typical behaviour of authorized users and processes. The basic difficulty facing researchers is that normal behaviour is highly variable based on a wide variety of innocuous factors. Many of the activities of intruders are indistinguishable from the benign actions of an authorized user.

The second major area of intrusion detection research is pattern recognition. The goal here is to detect patterns of network, host, and user activity that match known intruder attack scenarios. One problem with this approach is the variability that is possible within a single overall attack strategy. A second problem is that new attacks, with new attack patterns, cannot be detected by this approach.

## Approvals:

Name: Robert A Coats  
Title: Information Security officer

Signature:

Name: Claude LaPointe  
Title: IT director

Signature:

Name: Nilda Mejias  
Title: Computer Operations Manager

Signature:





PERFORMANCE WITH INTEGRITY

# Work from Home Policy

**Confidential**

Owner Kevin Odunga

## Summary of Changes

<b>Date</b>	<b>Issue</b>	<b>Description</b>	<b>Authorized by</b>
February 12, 2017	V1	Policy creation	Kevin Odunga
May 21, 2018	V2	Annual Review – no updates	Kevin Odunga
June 19, 2019	V3	Update to Technical Requirements – Anti-Virus	Kevin Odunga
March 20, 2020	V4	Update to minimum specifications for laptops	Kevin Odunga
May 5 <sup>th</sup> 2021	V4	NO changes.	Robert Coats

Last reviewed: May 5<sup>th</sup> 2021

Robert Coats

# REVIEW PROCESS: Annual review.

Date	Issue	Description	Authorized by
May 21, 2018	V2	Annual Review and update	Kevin Odunga
June 19, 2019	V3	Annual Review and update to Technical Requirements – Anti-Virus	Kevin Odunga
March 20, 2020	V4	Annual Review and update – Update to minimum specifications for laptops	Kevin Odunga
May 5 <sup>th</sup> 2021	V5	Changes to align with new policy. Many changes to requirements.	Robert Coats

Last reviewed: May 5<sup>th</sup> 2021

## **Policy**

It is policy to permit users remote access to Gatestone's information subject to authorization, procedures and security precautions.

## **Overview**

This guideline is intended to provide a framework for providing home users with a productive, flexible remote work environment that will satisfy our client's security requirements and maintain the same efficiency and reliability our on-premise agents experience.

## **Requirements**

### **Workspace Requirements**

#### **Workspace Requirements (Physical)**

- A secluded distraction-free working area with an ergonomic desk, ergonomic chair, and door - Commit a separate room/space for the home office away from household traffic patterns and lures.
- A quiet and uninterrupted workspace (no background noises that can hinder customer interactions)
- The workspace must have adequate heating and lighting
- Secure environment: take reasonable precautions necessary to secure the company's equipment.
- The user will arrange for Internet service with a direct connection to a cable or fiber optic modem, and a minimum 50 Mbps download and 10 Mbps upload. Speed tests will be performed to ensure the minimum requirements are met.
- Pay attention to your sight lines – ensure others cannot view your screen or keyboard.
- Workstation can either connect via Ethernet (preferred) to the home modem or is in good proximity with their Wi-Fi network
- Provide a picture of the WFH environment

#### **Technical Requirements (Logical)**

As per the baseline image approved by , Gatestone will provide a Endpoint that meets the following minimum-security requirements which will include:

- Employee's are to use secure wireless WPA 2 or more secure. They are to use WEP.
- Anti-virus and anti-malware software that follows all policy and is remotely monitored.
- Wyse Terminal will have Sophos web filter installed which follows policy

- Wyse Terminal will be fully disk encrypted with a BIOS password
- Follow all Gatestone password and authentication protocols
- Administrator access is removed for all users to prevent users from installing software.
- SCCM server will be used to update / install applications or updates on the user workstation remotely.
- Disable use of remote storage devices including all USB, Floppy, CDROM's, Printers or Scanners.
- Remove all copy and paste functions including snip tool via Active directory
- All GPO policy is to apply to WFH endpoints. This includes disabling of camera and microphone until approved by client.
- All remote access to the WFH endpoint will be removed including but not limited to RDP, Intelli-admin and other protocols from within Gatestone
- Geolocation filter in place to only allow connections from within Canada and or US and not offshore
- Softphones may be used but supplied by Gatestone
- Physical phones (Grandstream) are WiFi enabled with Transport Layer Security (TLS) for the connection between the phone and the Hosted PBX over Internet.
- A headset for the agents to use at home or in office.
- Below are the minimum specifications of the laptop.

1. **CPU: Intel Core i5-6200U**
2. **GPU: Intel HD Graphics 520**
3. **DISPLAY: 15.6", HD (1366 x 768), TN**
4. **STORAGE: 500GB SSD**
5. **RAM: 1x 12GB DDR3**
6. **WEIGHT: 2.45 kg (5.4 lbs)**

- The use of equipment and software, when provided by the company for use at the remote work location, is limited to authorized persons and for purposes relating to company business. The company will provide for repairs to company equipment.

### **Multifactor authentication details (Logical security)**

- Remote access via VPN requires 2 factor authentications. WatchGuard AuthPoint MFA will be used with an application installed on the employee's phone. Authentication will be enabled with a "Push" to the users' cell phone.
- Network will have a Radius server which Syncs with Active directory and the WatchGuard Cloud for control and logging MFA authentications
- Daily review of logs is required to verify
- Cisco AnyConnect VPN software is to be installed by the help desk with the configuration supplied by the network administrator for encryption.
- Remote laptops using the VPN must be registered to the Gatestone domain with the appropriate RADIUS server and the WFH group..

### **VPN Tunnel Details:**

- Dedicated VPN and NO Split tunneling allowed
- Authentication will be with via an IPSEC tunnel using SHA-256 with AES 256 encryption for Phase 1 and Sha-256/AES 256 with DH group 5 for Phase 2.
- Rules for access will be directly to the Gatestone network with only the ports needed for Citrix VDI, Teams and support applications (like AD, WSUS, AV etc.) are fully documented.
- All authentication logs will be kept for 6 months

### **Data Privacy**

- Employees are responsible for ensuring the security of the company's property and all client's information, files, documents, data, etc. within their possession, including both paper and electronic material. Staff should discuss the security implications of working from home with their local IT team.
- It will not be necessary for employees to transfer private or confidential information from the company intranet to home as these files should be stored and accessed by using either: Citrix or VMware to remotely access the data using the virtual desktop or terminal server where the data is held securely and any communication over the internet is encrypted both of these methods avoid the need to store any data on the local computer.
- Access to the network is controlled through two-factor authentication.

### **Personnel Security and security awareness**

- All users who work from home must be approved by their manager and security in writing.
- Employees are responsible for ensuring the security of the company's property and all client's information. Staff should discuss the security implications of working from home with their local IT team. Employees must NOT have any files / documents at home either physical or electronic. In the event of losing a WYSE terminal, they should immediately report to Gatestone Helpdesk and request a new one.
- Gatestone reserves the right to inspect the home work area to ensure compliance to policy.
- It will not be necessary for employees to transfer private or confidential information from the company intranet to home as these files should be stored and accessed by using either: Citrix or VMware to remotely access the data using the virtual desktop or terminal server where the data is held securely and any communication over the internet is encrypted both of these methods avoid the need to store any data on the local computer.
- Immediately report any lost or stolen laptops or through the Enterprise Incident Response Program (EIRP).
- Connect to the Gatestone network immediately after connecting the VPN, and sign off your computer when you step away.
- Store your computer and in a secure location.
- Accept all updates that are pushed to your computer.

- Do not use personal devices to conduct Gatestone business.
- Do not use computer devices for personal purposes
- Workstations and devices must be locked or logged off when unattended

Avoid discussing sensitive information where individuals can hear.

### **Virtual Desktop Interface (VDI) access**

- Remote access via VDI requires 2-factor authentication
- VDI prohibits cut, copy, paste functions from a Gatestone source to a remote computer.

### **3<sup>rd</sup> Party access**

Any 3<sup>rd</sup> party access is prohibited and if necessary must be authorized by Gatestone IT Security specialist prior to using subject to approved terms of use agreement between Gatestone and the 3<sup>rd</sup> party indicating security controls applicable in the circumstances.

Origin Date: July 26, 2013  
Updated: March 16, 2022

## **SUBJECT: HIPAA Confidentiality and Systems Usage Breach Policy**

**POLICY:** Workforce Members must protect patient and business information at all times. This policy outlines a consistent process for managing breaches of confidentiality and inappropriate use of information systems.

### **SUMMARY OF CONFIDENTIALITY AND SYSTEMS USAGE CONDUCT:**

Confidential Information – whether communicated verbally or by handwriting, printed paper, or electronic (from a computer) format – must be accessed and disclosed only to specifically support a patient care need, a business need, a legal need, or with the express written authorization of the patient or his/her legal representative.

Workforce members must seek and disclose the minimum amount of Confidential Information necessary to carry out their duties. Access to the records of family members, friends, co-workers, or other individuals is strictly prohibited (unless there is a job-related need).

All system access must be under each individual's own ID; sharing of passwords or doing work under someone else's account is a violation of law and policy. Workforce members are responsible for all activity recorded under their own IDs.

**Special laws require the most restrictive degree of confidentiality for mental health, substance abuse, certain infectious disease information and patients requesting to opt out of the facility directory.**

Note, the Appendix of this policy includes Key Definitions and guidelines regarding certain infectious disease information that may elevate the severity of a breach of confidentiality.

### **PROCEDURE**

Potential breaches identified by audit trail triggers, occurrence reporting, client or customer complaints, or any other means are reviewed and investigated by appropriate personnel. A breach is deemed to have occurred when any of the following conditions are met:

- Non job-related **access** to Protected Health Information (PHI) or other Confidential Information (that is, accessing Confidential Information without a job-related need to know); note, however, it is not a breach of confidentiality for individuals with access to hospital information systems to access their own electronic records;
- Non job-related **disclosure** of PHI or other Confidential Information (that is, sharing Confidential Information with someone else without a job-related need to know/disclose);
- An **invasion** of a patient's right to Privacy (that is, creating situations in which you might learn more about a patient's health information than is/was necessary to do your job, such as visiting a co-worker without the co-worker's permission upon work-related discovery of their admission/visit);

- A **violation of Information Security policies**, for example, allowing a co-worker to access information under your individual ID

Incidents meeting any of these criteria are deemed a breach of confidentiality, security, and/or a violation of information systems usage policy and will be subject to corrective action in accordance with this policy.

Through the course of investigation, if it is evident that there was a business-related (legitimate) need for the disclosure, the investigation will end and no corrective action will be necessary. Otherwise, the breach will be referred to the Security Review Committee (SRC) for evaluation and/or a recommended course of action in a timely manner. The Security Review Committee is a committee comprised of the following Gatestone personnel: CEO, President, Executive Vice President, Chief Compliance Officer and Information Security Officer.

Every breach of confidentiality, security, and/or violation of information systems usage policy introduces the potential for corrective action. When determining appropriate corrective action for a given violation, three primary factors are considered.

1. The Workforce Member's intent in seeking, accessing, using, and/or disclosing Confidential Information. Intent need not be absolutely proven to enforce sanctions; apparent intent may be determined by the judgment of the SRC based on known facts and circumstances.
2. The level of the potential or actual damage/harm caused by the violation, including potential or actual legal or regulatory implications for Gatestone, etc., as determined by the SRC.
3. Whether PHI more restrictive in nature (mental health, substance abuse, sensitive infectious disease information, and patients requesting to opt out of the facility directory) was breached. **Breaches of this type will automatically result in Major level of harm.**

In the case of any sanction imposed on an employee, if corrective action already exists in the employee's personnel file, then the corrective action issued under this policy will be escalated in accordance with existing corrective action policies.



Violations and resulting sanctions are categorized based on the following definitions:

PRIVACY AND SECURITY INCIDENT SEVERITY SCALE GUIDELINE WITH RECOMMENDED DISCIPLINARY ACTIONS				
LEVEL OF HARM				
		NEGLIGIBLE No effect on patient or organization; no apparent risk	MINOR/MODERATE Minor or moderate harm (or potential harm) to patient, groups of patients and/or organization	MAJOR Major harm (or potential harm) to patient, groups of patients and/or organization
<b>INTENT</b>	<b>UNINTENTIONAL:</b> No known or believed intent; or inadvertent mistake; or carelessness  <b>Additional Considerations</b> <ul style="list-style-type: none"> <li>• Previous violations of confidentiality or systems usage?</li> <li>• User error/ lack of understanding of the IS application?</li> <li>• Lack of adequate job-specific training?</li> <li>• Could not possibly have known?</li> <li>• Following supervisor's directive?</li> </ul>	1	1	2
	<b>INTENTIONAL:</b> Due to curiosity or concern; or negligence  <b>Additional Considerations</b> <ul style="list-style-type: none"> <li>• Previous violations of confidentiality or systems usage?</li> <li>• Lack of adequate job-specific training?</li> </ul>	2	3	4
	<b>INTENTIONAL:</b> Malicious intent including use of info in a domestic dispute; Personal financial gain; Willful or reckless disregard of policies, procedures or law.	4	4	4
<b>DISCIPLINARY RECOMMENDATIONS:</b> 1 (White): No Action, or a Verbal or a Written Warning; 2 (Yellow): Written Warning or Final Written Warning; 3 (Orange): Final Written Warning, Suspension (or equivalent) or Termination; 4 (Red): Termination.				

Sanctions are carried out as follows.

For employees, the CEO and/or President will work with the employee/user's manager and the Human Resources department, when necessary, to implement the sanctions. Managers must seek their administrator's approval if they feel that mitigating circumstances justify a less severe corrective action. Employee corrective action and appeal requests will be handled in accordance with existing corrective action policies and procedures. The final determination of terminating an employee will involve the employee's Manager and a representative of Human Resources. Any exceptions to the disciplinary action recommended by the Security Review Committee must be approved by the CEO.

**APPENDIX:  
KEY DEFINITIONS**

**Confidential Information** constitutes either of the following:

**Business Information:** Any information regarding the business and operations of Gatestone or any of Gatestone's clients or customers obtained during the course of your work. This may include, but is not limited to, information concerning employees, physicians, financial operations, quality assurance, utilization review, risk management, research, procurement, contracting, and other operational information.

**Protected Health Information** ("PHI") means information that: (i) is created or received by a Health Care Provider, Health Plan, or Health Care Customer; (ii) relates to the past, present or future physical or mental health or condition of an Individual; the provision of Health Care to an Individual, or the past, present or future Payment for the provision of Health Care to an Individual; and (iii) identifies the Individual (or for which there is a reasonable basis for believing that the information can be used to identify the Individual).

**Workforce** or **Workforce Member** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Facility, is under the direct control of such Entity, whether or not they are paid by the Facility.

**Certain Infectious Disease Information:** Public Health Laws have been invoked from time to time when there is improper access to or disclosure of protected health information relating to a patient's infectious disease, when the improper access or disclosure causes great harm (or the potential for great harm) to that person. Diseases such as sexually transmitted diseases (STDs) can cause harm to patients if the information is disclosed beyond patient care needs.



## 4. Cost Proposal

Our Cost Proposal is contained in a separate Excel document.



## VII. Attachments

## 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:	Gatestone & Co. International, Inc.
Bidder Address:	7015 L Street, Omaha, NE 68117
Contact Person & Title:	Spencer Wilson, Senior Vice President
E-mail Address:	spencer.wilson@gatestonebpo.com
Telephone Number (Office):	1-800-900-4238 x 2993
Telephone Number (Cellular):	602-424-6455
Fax Number:	602-443-2929

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:	Gatestone & Co. International, Inc.
Bidder Address:	7015 L Street, Omaha, NE 68117
Contact Person & Title:	Spencer Wilson, Senior Vice President
E-mail Address:	spencer.wilson@gatestonebpo.com
Telephone Number (Office):	1-800-900-4238 x 2993
Telephone Number (Cellular):	602-424-6455
Fax Number:	602-443-2929

**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.

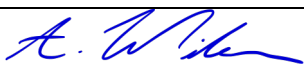
Per Nebraska's Transparency in Government Procurement Act, Neb. Rev Stat § 73-603 DAS is required to collect statistical information regarding the number of contracts awarded to Nebraska Contractors. This information is for statistical purposes only and will not be considered for contract award purposes.

**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:	<b>Gatestone &amp; Co. International, Inc.</b>
COMPLETE ADDRESS:	<b>7015 L Street, Omaha, NE 68117</b>
TELEPHONE NUMBER:	<b>480-652-4440</b>
FAX NUMBER:	<b>602-443-2929</b>
DATE:	<b>December 6, 2022</b>
SIGNATURE:	
TYPED NAME & TITLE OF SIGNER:	<b>Alexander Wilson, Vice President</b>

**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:

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:
A.W.			

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:
A.W.			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
A.W.			

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:
A.W.			

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:
A.W.			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

**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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
A.W.			

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:
A.W.			

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 Contractor, 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:
A.W.			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
A.W.			

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:
A.W.			

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:
A.W.			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
A.W.			

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:
<i>A.W.</i>			

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:
<i>A.W.</i>			

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:
A.W.			

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.



GATESTONE  
*bpo*

**ATTACHMENT 4  
COST PROPOSAL SHEET**

**Bidder Name** **Gatestone & Co. International, Inc.**

**ONE TIME COST**

Startup Plan/Implementation Cost **\$0.00**

**PASS THROUGH COSTS**

Cost per page, single sided printing **\$0.1925**

Training Cost Per Hour/Per Person **\$21.00**

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	\$ 16.13	17,000-27,999	\$ 16.13	28,000-40,000	\$ 16.13
	B	15:01-20:00	1,400-3,599	\$ 16.13	3,600-5,799	\$ 16.13	5,800-8,000	\$ 16.13
	C	20:01-25:00	1,400-3,599	\$ 16.13	3,600-5,799	\$ 16.13	5,800-8,000	\$ 16.13
	D	25:01-30:00	1,400-3,599	\$ 16.13	3,600-5,799	\$ 16.13	5,800-8,000	\$ 16.13
	E	30:01-35:00	1,400-3,599	\$ 16.13	3,600-5,799	\$ 16.13	5,800-8,000	\$ 16.13
<b>Outreach</b>	A	8:00 -12:00	1,400-3,599	\$ 16.13	3,600-5,799	\$ 16.13	5,800-8,000	\$ 16.13
	B	12:01 - 16:00	1,400-3,599	\$ 16.13	3,600-5,799	\$ 16.13	5,800-8,000	\$ 16.13
	C	16:01 - 20:00	1,400-3,599	\$ 16.13	3,600-5,799	\$ 16.13	5,800-8,000	\$ 16.13
<b>Back Office Processing</b>	A	4:00-8:00	1,400-3,599	\$ 15.61	3,600-5,799	\$ 15.61	5,800-8,000	\$ 15.61

B	8:01 - 12:00	1,400-3,599	\$ 15.61	3,600-5,799	\$ 15.61	5,800-8,000	\$ 15.61
C	12:01-16:00	1,400-3,599	\$ 15.61	3,600-5,799	\$ 15.61	5,800-8,000	\$ 15.61

**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
<b>Inbound</b>	A	11:00-15:00	6,000-16,999	\$ 16.94	17,000-27,999	\$ 16.94	28,000-40,000	\$ 16.94
	B	15:01-20:00	1,400-3,599	\$ 16.94	3,600-5,799	\$ 16.94	5,800-8,000	\$ 16.94
	C	20:01-25:00	1,400-3,599	\$ 16.94	3,600-5,799	\$ 16.94	5,800-8,000	\$ 16.94
	D	25:01-30:00	1,400-3,599	\$ 16.94	3,600-5,799	\$ 16.94	5,800-8,000	\$ 16.94
	E	30:01-35:00	1,400-3,599	\$ 16.94	3,600-5,799	\$ 16.94	5,800-8,000	\$ 16.94
<b>Outreach</b>	A	8:00 -12:00	1,400-3,599	\$ 16.94	3,600-5,799	\$ 16.94	5,800-8,000	\$ 16.94
	B	12:01 - 16:00	1,400-3,599	\$ 16.94	3,600-5,799	\$ 16.94	5,800-8,000	\$ 16.94
	C	16:01 - 20:00	1,400-3,599	\$ 16.94	3,600-5,799	\$ 16.94	5,800-8,000	\$ 16.94
<b>Back Office Processing</b>	A	4:00-8:00	1,400-3,599	\$ 16.39	3,600-5,799	\$ 16.39	5,800-8,000	\$ 16.39
	B	8:01 - 12:00	1,400-3,599	\$ 16.39	3,600-5,799	\$ 16.39	5,800-8,000	\$ 16.39
	C	12:01-16:00	1,400-3,599	\$ 16.39	3,600-5,799	\$ 16.39	5,800-8,000	\$ 16.39

**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
<b>Inbound</b>	A	11:00-15:00	6,000-16,999	\$ 17.78	17,000-27,999	\$ 17.78	28,000-40,000	\$ 17.78
	B	15:01-20:00	1,400-3,599	\$ 17.78	3,600-5,799	\$ 17.78	5,800-8,000	\$ 17.78
	C	20:01-25:00	1,400-3,599	\$ 17.78	3,600-5,799	\$ 17.78	5,800-8,000	\$ 17.78
	D	25:01-30:00	1,400-3,599	\$ 17.78	3,600-5,799	\$ 17.78	5,800-8,000	\$ 17.78
	E	30:01-35:00	1,400-3,599	\$ 17.78	3,600-5,799	\$ 17.78	5,800-8,000	\$ 17.78
<b>Outreach</b>	A	8:00 -12:00	1,400-3,599	\$ 17.78	3,600-5,799	\$ 17.78	5,800-8,000	\$ 17.78
	B	12:01 - 16:00	1,400-3,599	\$ 17.78	3,600-5,799	\$ 17.78	5,800-8,000	\$ 17.78
	C	16:01 - 20:00	1,400-3,599	\$ 17.78	3,600-5,799	\$ 17.78	5,800-8,000	\$ 17.78
<b>Back Office Processing</b>	A	4:00-8:00	1,400-3,599	\$ 17.21	3,600-5,799	\$ 17.21	5,800-8,000	\$ 17.21
	B	8:01 - 12:00	1,400-3,599	\$ 17.21	3,600-5,799	\$ 17.21	5,800-8,000	\$ 17.21
	C	12:01-16:00	1,400-3,599	\$ 17.21	3,600-5,799	\$ 17.21	5,800-8,000	\$ 17.21

### 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	\$ 18.67	17,000-27,999	\$ 18.67	28,000-40,000	\$ 18.67
	B	15:01-20:00	1,400-3,599	\$ 18.67	3,600-5,799	\$ 18.67	5,800-8,000	\$ 18.67
	C	20:01-25:00	1,400-3,599	\$ 18.67	3,600-5,799	\$ 18.67	5,800-8,000	\$ 18.67
	D	25:01-30:00	1,400-3,599	\$ 18.67	3,600-5,799	\$ 18.67	5,800-8,000	\$ 18.67
	E	30:01-35:00	1,400-3,599	\$ 18.67	3,600-5,799	\$ 18.67	5,800-8,000	\$ 18.67
<b>Outreach</b>	A	8:00 -12:00	1,400-3,599	\$ 18.67	3,600-5,799	\$ 18.67	5,800-8,000	\$ 18.67
	B	12:01 - 16:00	1,400-3,599	\$ 18.67	3,600-5,799	\$ 18.67	5,800-8,000	\$ 18.67
	C	16:01 - 20:00	1,400-3,599	\$ 18.67	3,600-5,799	\$ 18.67	5,800-8,000	\$ 18.67
<b>Back Office Processing</b>	A	4:00-8:00	1,400-3,599	\$ 18.07	3,600-5,799	\$ 18.07	5,800-8,000	\$ 18.07
	B	8:01 - 12:00	1,400-3,599	\$ 18.07	3,600-5,799	\$ 18.07	5,800-8,000	\$ 18.07
	C	12:01-16:00	1,400-3,599	\$ 18.07	3,600-5,799	\$ 18.07	5,800-8,000	\$ 18.07