Information Security Management Program

Sterling Associates Incorporation recognizes the criticality of preserving the integrity of its platform to safeguard customer information. To achieve this goal, we have established the Information Security Management Program (ISMP). The primary objective of this program is to implement industry best practices and adhere to applicable rules and regulations.

Table of Content

General Overview

This policy benefits entities by establishing a framework to guarantee the implementation of appropriate measures for safeguarding the confidentiality, integrity, and availability of data. It also ensures that staff and all other affiliates comprehend their roles and responsibilities, possess adequate knowledge of security policies, procedures, and practices, and are proficient in protecting information.

The policy outlines the general overview of this program as follows:

- Sterling Associates Inc is committed to protecting the confidentiality of customer data, including contact information, message content, and campaign details. We implement robust access controls, encryption technologies, and secure storage practices to ensure that only authorized personnel have access to sensitive information.

- Sterling Associates Incorporation maintains the accuracy and completeness of customer data throughout its lifecycle. This includes employing data validation techniques, preventing unauthorized data modification, and implementing intrusion detection systems to safeguard against cyberattacks.

- Sterling Associates Inc prioritizes the uninterrupted availability of our SMS platform. We utilize redundant infrastructure, disaster recovery plans, and regular system maintenance to ensure continuous operation and minimize downtime.

- All Sterling Associates Inc personnel are accountable for upholding information security practices. This includes adhering to security policies, attending security awareness training, and promptly reporting any suspected security incidents.

Security Practices

The security practices of Sterling Associates Incorporations Information Security Management Program (ISMP) is central to our dedication to information security and earning customer trust. Through these robust policies and procedures, we ensure a secure and dependable SMS platform for our clients. We are committed to continually enhancing our security measures to address evolving threats effectively.

- We implement detailed access controls to restrict access to customer data and system resources, adhering to the principle of least privilege. Additionally, multi-factor authentication is required for all privileged accounts.

- We encrypt sensitive data using industry-standard algorithms, both at rest and in transit, to prevent unauthorized access even in the event of a security breach.

- Our systems and applications undergo regular vulnerability assessments, including penetration testing and patch management, to mitigate security risks.

- Sterling Associates Inc has a well-defined incident response plan that guides our actions in detecting, containing, eradicating, and recovering from security breaches. This plan includes protocols for timely communication with affected customers and regulatory bodies.

- Employees receive ongoing training on information security best practices, covering topics like recognizing security threats and their role in maintaining a secure environment.

- Before granting access to customer data or our platform, all third-party vendors undergo comprehensive security assessments. Contracts with third-party service providers include security clauses to ensure adherence to our standards.

- Sterling Associates Inc follows data retention policies compliant with regulations and industry standards. Customer data is securely disposed of after the designated retention period.

Roles and Areas of Responsibility

Sterling Associates Inc prioritizes the security and integrity of all information assets, both physical and electronic. To achieve this objective, we have established a clear delineation of roles and responsibilities, ensuring effective information security management in accordance with current laws, regulations, and contractual requirements.

Executive Oversight

- **The Chief Executive Officer (CEO)** bears ultimate responsibility for Sterling Associates Incs information security posture. This encompasses information security regarding personnel and IT systems. Additionally, the CEO and Executive Team own the Information Security Policy, approving and signing off on any policy changes.

- **The Chief Information Officer (CIO)** holds primary responsibility for ensuring the implementation and effectiveness of information security measures across Sterling Associates Inc.

System Ownership

- The **System Owner i**n collaboration with the IT department is responsible for all aspects of information security within their domain. This includes defining purchasing requirements, development activities, and maintenance procedures for information systems and related data. Each system and information type must have a designated owner. The System Owner main Responsibilities includes:

    - Defining authorized users or user groups who can access specific information.

    - Determining the appropriate use of the entrusted information.

System Administration

- System Administrators at Sterling Associates Inc are responsible for overseeing the administration of our information systems and managing data entrusted by third parties. They may specialize in specific types of information or systems to ensure efficient operation.

- These professionals enforce access control measures to protect information confidentiality and perform routine backups to maintain the availability and integrity of critical data across our network.

User Responsibility

- All Sterling Associates Inc employees are responsible for familiarizing themselves with and complying with established information technology regulations. Any questions regarding the handling of various information types should be directed to the designated system owner or system administrator.

Risk and governance policy

Sterling Associates Inc places a high priority on information security. We recognize that threats to your data and our systems are always changing. This is why we take a proactive approach, regularly assessing risks to ensure your information stays safe.

- Sterling Associates Inc conducts comprehensive risk assessments of our entire information system ecosystem on a yearly basis. These assessments apply to every aspect of our systems, identifying vulnerabilities and potential threats.

- Our assessments go beyond simply identifying threats. We leverage established criteria to quantify the severity of each risk, allowing us to prioritize our efforts and allocate resources effectively. This ensures that we address the most critical issues first.

- All risk assessments are thoroughly reviewed and approved by Sterling Associates Incorporations management team, including the system owners who possess deep understanding of specific systems. This collaborative approach guarantees that risk assessments are aligned with our overall security strategy and business objectives.

- If a risk assessment identifies a threat deemed unacceptable, we take swift action. We implement a tailored set of defensive measures to mitigate the risk and bring it down to an acceptable level. This ensures the continued security of your data and the smooth operation of our systems.

Access Management with IT access control and user access policy

This policy establishes the general principles and guidelines for Access Management. Sterling Associates Inc maintains an access control policy that describes how to manage access to systems, the basic principles include:

- We utilize secure user accounts and passwords to manage access to our systems. This ensures only authorized personnel can log in and view sensitive data.

- We take data security seriously, but you play a vital role too. It's every user's responsibility to manage their access credentials carefully and report any suspicious activity.

- Our systems are constantly monitored and logged for potential security breaches. This allows us to identify and address any unauthorized access attempts promptly.

- When accessing Sterling Associates Inc systems remotely, AWS security groups ensure only authorized connections are established. This adds an extra layer of protection for your data.

- We follow the principle of "least privilege" and "strict need to know." This means access to Sterling Associates Inc systems is granted based on a user's specific role and responsibilities. They will only have access to the information they absolutely need to perform their tasks.

Asset Management

Sterling Associates Inc's Information Technology Asset Management Policy promotes a culture of responsibility and accountability for IT assets. This policy establishes the general principles and guidelines for the management of Sterling Associates Inc IT assets and how those assets should be handled.

- It states that Sterling Associates Inc maintains a meticulous and up-to-date inventory of all IT assets. This inventory encompasses hardware (such as desktops, laptops, servers, and network devices), software (including licensed applications and operating systems), and any other IT resources utilized within our organization. *The inventory details the specific characteristics, location, and ownership of each asset, allowing for efficient tracking and management.*

- Each IT asset within the Sterling Associates Inc ecosystem has a clearly identified owner. This owner is responsible for the asset's security, proper use, and adherence to company policies. By assigning ownership, we foster accountability and ensure that all assets are actively monitored and managed.

- Sterling Associates Inc has established clear guidelines for the acceptable use of IT assets. These guidelines outline the permitted activities and applications for each asset type. This fosters responsible use and helps prevent unauthorized activities that could compromise data security or system integrity.

- Upon employee termination, all Sterling Associates Inc-issued IT assets must be returned to the designated IT department. This ensures the proper tracking and control of all assets, minimizing the risk of loss or unauthorized use.

Business continuity and disaster recovery

This policy establishes the general principles of our approach towards resilience, availability and continuity of processes, systems and services at Sterling Associates Inc. It defines requirements around business continuity, disaster recovery, and crisis management processes. The basic principles for business continuity and disaster recovery entails the follows:

- Owners of mission-critical systems, processes or services must ensure adequate business continuity and / or disaster recovery that is in line with tolerance for disruption in the event of a disaster.

- Continuity plans must include an appropriate "last support" environment, providing basic functionality (at a minimum), and a plan to fail in that environment. Considerations for resuming normal business should also be included.

- No mission-critical system, process, or function should be deployed into a production environment without a proper continuity plan.

- Plans should be tested quarterly and issues identified and addressed.

- Recovery Time Objective (RTO) starts from event detection until core functionality is operational. The services are grouped into tiers that define the maximum RTO.

Communications security

Sterling Associates Inc establishes the general principles and guidelines for managing the security of our communication channels and networks as well. There are certain principles that users needs to comply:

- Access to our network is strictly controlled. This means only authorized users and devices can gain entry, preventing unauthorized access and potential data breaches.

- When network access is granted, it's crucial for users to understand their responsibilities. This includes familiarity with the Global Electronic Systems and Communications Policy, ensuring everyone plays a part in maintaining a secure environment.

- Sterling Associates Inc implements network segmentation based on criticality. This means highly sensitive data resides in its own secure network segment, further limiting unauthorized access attempts.

Encryption and cipher

This policy establishes the general principles to ensure that Sterling Associates Inc implements appropriate encryption and cryptography to ensure the confidentiality of critical data. Sterling Associates Inc implements cryptographic mechanisms to mitigate the risks involved in the storage of sensitive information and its transmission through networks, including those that are publicly accessible (such as the Internet).

Sterling Associates Inc will ensure:

- Sensitive data is properly encrypted.
- The strength of the selected encryption corresponds to the categorization of the information.
- Cryptographic keys will be managed securely.
- Only approved cryptographic algorithms will be used.
- That system connections with clients and operators are always through VPN tunnel or TLS / SSL.

Data security and information life cycle management

The Data Security Classification Policy sets out the general requirements on how to handle customer data. Examples of how to handle different types of data can be found below. All employees should consider how to handle both internal and customer data.

All employees share the responsibility to ensure that our information receives an adequate level of protection by observing this Information Classification policy:

- The information must be classified in terms of legal requirements, value and criticality for Sterling Associates Inc.
- Information should be labeled to ensure proper handling.
- Manage all removable media with the same handling guidelines as below.

- Media that is removed must be safely removed.

- Media containing company information must be protected against unauthorized access, misuse, or corruption during transportation.

Mobile and bring your own device

This Policy establishes the general principles and guidelines for the use of personal devices with Sterling Associates Inc networks and environments.

This Bring Your Own Device (BYOD) Policy is intended to be as discreet and flexible as possible regarding the use of BYOD to maintain the autonomy of employees and ensure that we have the ability to protect our customers and corporate data.

The primary focus will be on configuration / posture verification and device compliance monitoring, with the least restrictive principles that reasonably achieve the required security objectives, rather than applying restrictions.

When restrictions need to be applied, this will be done selectively depending on the data that can be accessed.

This Policy covers our current and anticipated future needs. Some of the capabilities described may not be immediately implemented.

Operations

This Operations Policy outlines the foundation for how Sterling Associates Inc manages its technological infrastructure. This document details core principles designed to ensure smooth and reliable functioning of our systems. These principles include establishing documented procedures, maintaining regular and tested backups, implementing a multi-person change approval process, and proactively planning for capacity needs.

- Sterling Associates Inc procedures will be documented for operational activities.

- Our backups will be taken regularly and tested.

- All changes will be managed and evaluated by several people.

- Capacity must be assessed and planned to

- Software installation must be limited and unnecessary software must be restricted.

- Logs must be configured and forwarded to the centralized logging platform.

- Any operational incident must be managed according to our common incident.

Physical and Environmental Security

Sterling Associates Inc recognizes the importance of protecting both the data and the physical environment where it resides. This policy outlines our commitment to physical and environmental security, ensuring the safety of our personnel, buildings, equipment, and ultimately, the integrity of your information.

Here's what this means for you:

- Sterling Associates Inc provides a safe and secure work environment for our employees and any authorized visitors. This includes maintaining well-lit and hazard-free facilities, along with appropriate security measures to deter unauthorized access.

- We understand the critical role IT equipment plays in our operations. SAI implements robust security measures to safeguard this equipment, whether it's located within our offices or at remote data centers. These measures may include physical access controls, video surveillance, and environmental monitoring systems.

- Access to Sterling Associates Inc buildings and offices is restricted to authorized personnel only. This may involve the use of secure keycard systems, access logs, and visitor management protocols. These measures help us maintain a controlled environment and minimize the risk of unauthorized access to sensitive information or equipment.

Privacy

This policy establishes the general principles for managing the privacy of customer-related data. The basic principles includes:

- Manage controls around the collection of customer data.
- Customer data review should be kept for support purposes only.
- The only scenarios in which customer data can be cloned are for backup or support purposes.

Apart from that, Sterling Associates Inc is committed to complying with all applicable data privacy regulations, including but not limited to:

- ***General Data Protection Regulation (GDPR) (if applicable)***
- ***California Consumer Privacy Act (CCPA)***

Security incident management

This policy establishes the general principles and guidelines to ensure that Sterling Associates Inc reacts appropriately to any actual or suspected security incident. Sterling Associates Inc has the responsibility of monitoring incidents that occur within the organization that may violate the confidentiality, integrity or availability of information or information systems. All suspicious incidents must be reported and evaluated.

Sterling Associates Incorporations security team will:

- Anticipate security incidents and prepare corresponding response plans.
- Contain, eradicate and recover from any incident.
- We will invest in our people, processes and technologies to ensure that we have the ability to detect and analyze an incident when it occurs.

- When responding to an incident, we will put the protection of customer data as our top priority.

Data management of suppliers and third parties

This policy establishes the general principles and guidelines to select, involve and monitor the provider's access to Sterling Associates Inc data.

Sterling Associates Inc will ensure:

- A purpose in managing our supplier selection process.

- The business owner requesting the supplier relationship is responsible for using Sterling Associates Incorporations standard contracts.

- Monitoring the relationship to ensure it meets our Sterling Associates Inc standards.

- We reserve the right to terminate the contract with any provider when the service is no longer needed.

Acquisition, development and maintenance of the system

This policy establishes the general principles and guidelines for application development, both internal and customer-oriented, as well as creates limitations on how to manage the pre-production environment and incorporate open-source software in any of our products.

The basic principles include:

- Security requirements will be included and incorporated into any environment or application development or acquisition.

- Product development will follow our internal quality assurance process, which includes the integration of security controls.

- Production data will be anonymized or masked when used in pre-production environments.

- The integration of any open-source framework or library will follow our internal guidelines.

Threat and vulnerability management

Sterling Associates Inc recognizes malware as a particularly pervasive threat and will employ robust detection and mitigation strategies to protect our systems and data. We are committed to a rigorous Threat and Vulnerability Management (TVM) program that safeguards both our internal infrastructure and the security posture of the products and services we deliver.

We will manage the threat of malware in the environment by implementing comprehensive vulnerability scanning and penetration testing methodologies helps us to strive in eliminating potential security gaps (before they can be exploited)

We follow a structured approach for proactively identifying, assessing, and mitigating security threats and vulnerabilities where we will actively manage vulnerabilities within the products and services through a dedicated process for issuing timely updates, security patches, or advisories to address any discovered weaknesses.

This proactive approach extends to our entire environment, encompassing both internally managed systems and those hosted by third-party providers.

Audit and compliance management

This policy establishes the general principles and guidelines for managing the audit and compliance program to validate the implementation of Sterling Associates Inc Control Framework.

We implement technology-centric operations, security and privacy controls to ensure they comply with internal policies, regulations, and external industry standards.

Audits are coordinated and delivered as appropriate to achieve a high level of confidence in our control environment, as well as to achieve internal or external certification.

Sterling Associates Inc collaborates with all requests for external validation of the implementation of our operational, security, privacy and other controls.

Sterling Associates Inc maintains a consolidated view of all its relevant objectives, activities and tests of control.

Sterling Associates Inc
Information security management program

Approved by:	Ronald Seiler
Issued Date:	03rd July 2024