Sterling
Volunteers

Privacy and Information Security at Sterling Volunteers

Sterling Volunteers

Introduction

Sterling Volunteers takes significant measures to ensure the security and privacy of data in our custody. From encrypted databases and communication links, to regular review of information handling processes through Privacy Impact Assessments and ongoing security monitoring, Sterling Volunteers takes all appropriate technical and organizational measures to safely and responsibly store, transmit, and process information. A world-class, comprehensive privacy policy that applies to all personal information, as well as a layered security strategy that includes technical, procedural, and quality controls, ensures that all data is handled in the way our clients and their applicants expect.

Privacy

Privacy Mission Statement

Sterling Volunteers is committed to the protection of individual privacy rights. We hold ourselves to the highest legal and ethical standard for compliance and strive to be a privacy champion in the background screening industry. We value the trust placed in us by clients, colleagues and suppliers, and work to maintain that trust by building privacy protection into everything we do.

Core Privacy Principles

Accountability

We are accountable for our privacy practices. We are responsible for safeguarding the personal information entrusted to us. Sterling Volunteers has appointed a team of privacy professionals to ensure we comply with our Privacy Policy, the law, our contractual obligations and the rights of individuals. This team provides training and guidance on privacy matters and investigates concerns and complaints from colleagues, clients, individuals or government agencies. We take privacy concerns and complaints seriously and investigate and respond to them in good faith.

Fairness and Transparency

We handle personal information in line with individuals' expectations and the law.

We only collect and use personal information with the consent of the individual or where there is a legitimate purpose to do so. Individuals may withdraw consent for use of their personal information at any time.

Proportionality

We ensure that we collect, use and retain only the personal information we need for a specified purpose. We do this by observing a number of more specific principles:

- **Limiting Purposes.** We do not use personal information for purposes that are incompatible with those that were identified when the information was first collected, unless the individual has consented to the new purpose, or it is required by law.
- **Limiting Collection, Use and Disclosure.** We avoid the collection, use and disclosure of personal information that is not necessary for the purposes we have identified, unless required by law.
- **Retention.** We retain personal information long enough to fulfill the purpose for which it was originally collected, to fulfill our legal obligations, and to allow individuals to exercise their rights under the law. We securely destroy or anonymize personal information that we are no longer required to retain.

Sterling Volunteers

Quality and Accuracy

We take reasonable steps to ensure that personal information is accurate, complete and, where necessary, kept up to date.

We collect personal information directly from individuals, through intermediaries such as our clients, and from third parties. While we are not responsible for the accuracy of information held or provided by others, we have robust procedures in place to ensure personal information is recorded faithfully in our system and any errors are corrected promptly.

Security

We ensure personal information in our custody is kept secure. We take the necessary technical and organizational measures to ensure personal information is secured against accidental access, destruction, loss, modification or disclosure, and take appropriate steps to reduce or eliminate harm in case of a breach.

We do not transfer personal information to third parties or overseas when it is prohibited by law. When it is permitted to transfer personal information, we ensure that it continues to benefit from the protections afforded by our Privacy Policy and the laws that apply where it was collected.

Individual Participation

We help individuals understand and exercise their legal rights with respect to the personal information entrusted to us.

All individuals have the right to know whether we hold personal information about them and, if we do, how it has been or will be used and disclosed. They have a right to access personal information about themselves upon request, with reasonable limitations as provided by law. Individuals have the right to dispute the accuracy of their personal information and, if their dispute is successful, have their information updated as appropriate. We inform individuals about their rights upon request and as required by law and take reasonable steps to assist them in exercising those rights.

Privacy by Design

We build privacy into everything we do.

We subscribe to the concept of Privacy by Design. This means that we take a proactive approach to privacy. Rather than trying to fix privacy problems as they come up, we aim to prevent them entirely. Before a new system, product or procedure is developed, or an existing one is modified, we carefully review any effect it may have on personal information to ensure these Core Privacy Principles are upheld.

Privacy Audits

All Sterling Volunteers business units and functional areas that collect, use, disclose or store personal information are subject to annual internal audits for compliance with our Core Privacy Principles, as well as occasional spot checks in case of complaints or incidents. Privacy audit results and evidence documentation are centrally managed by our privacy team.

Information Security

External Infrastructure

The Sterling Volunteers application infrastructure follows best practice designs in ensuring the security of the web application environment. After authentication to access the Sterling Volunteers application, all transactions are carried over a 128-bit encrypted connection to the Web server, and application communications take place over a secure VLAN on the internal network. All data is stored in an encrypted database on fault tolerant storage. This

design allows for full confidentiality of all data by ensuring encryption while in transit between systems, as well as while it is at rest in our secured data center.

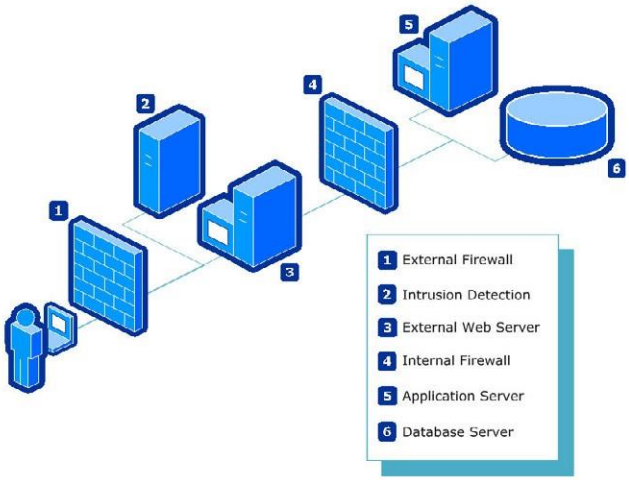

Figure 1: Strong External Security

Internal Infrastructure

Sterling Volunteers is committed to Information Security in all aspects of its operations, focusing not only on external systems but internal systems as well. Sterling Volunteers employs industry best practices in our software development processes, change management processes, and infrastructure management processes. Maintaining the integrity of the production operational environments is one of the primary focuses. To achieve that goal, the development, quality, and production environments are segregated from each other using both firewall and network segmentation technologies. This ensures that application developers can neither impact nor access the data and applications contained within the secured production segments.

Technology Operations

In the customer operations environment, Sterling Volunteers has implemented a robust and secure architecture that ensures continuing security and confidentiality of all data. By leveraging virtualization technology, secure application environments, and strong physical security controls, Sterling Volunteers has built an environment that protects all of the data under our control from loss.

When the time comes to return data to our clients, Sterling Volunteers takes the same measure of care that we take in protecting the data while under our control. Sterling Volunteers employs desktop protection that prevents copying of protected information and uses data loss prevention technology on outbound systems that is able to ensure that sensitive data is encrypted when being returned to our customers. This same technology monitors for the transmission of sensitive data and allows us to monitor for abnormal behavior.

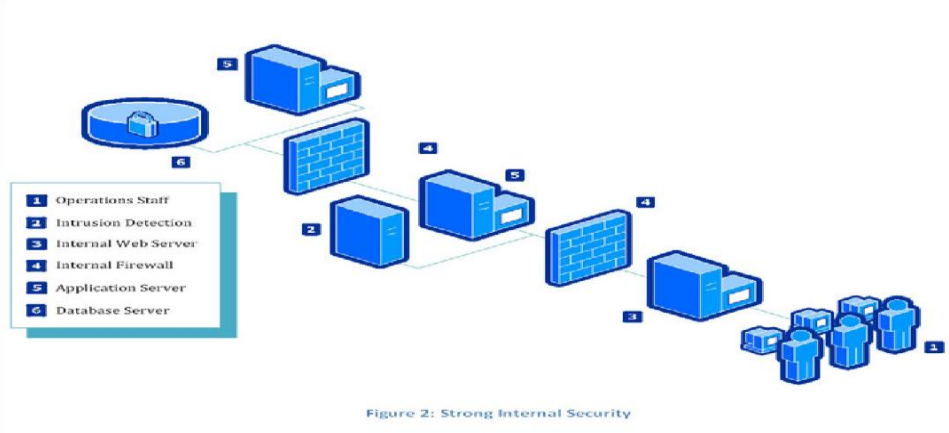

Figure 2: Strong Internal Security

Disaster Recovery

To ensure maximum availability for Sterling Volunteers' applications, Sterling Volunteers maintains multiple data centers in an active/standby relationship. The primary data center is responsible for normal operations, and in the event of a disaster, the alternate data center is on hot standby, ready to assume processing within a matter of hours.

Security Audits

To complement and verify our set of security controls, Sterling Volunteers undergoes three different audits with external auditors each year. External auditors perform a network perimeter security assessment, an application penetration test, and a physical security assessment at our key facilities. The results of these audits are then fed back into our Information Security Management System (ISMS).

The Sterling Volunteers ISMS is the set of processes used when assessing our compliance with the ISO 27001/27002 set of controls. Sterling Volunteers is an ISO 27001 certified organization. This means that an independent auditor, who has been accredited by the International Organization for Standardization (ISO), audits our compliance with our documented ISMS in conjunction with the ISO 27001/27002 controls and certifies our compliance with that standard.

Training and Enforcement

All Sterling Volunteers employees are required to complete several Privacy and Information Security training modules at the beginning of employment and annually thereafter. Training programs are tailored to job function and explain the importance and application of information security controls, the Core Privacy Principles and how to recognize and respond to incidents of non-compliance or potential breach. Each training module is followed by a short quiz to ensure understanding. Non-compliance with privacy and security policies results in disciplinary action and retraining or, in some cases, termination of employment.

Incident Response

While privacy or data security incidents are rare, Sterling Volunteers takes any report or suspicion of an incident seriously. A privacy incident is the unauthorized access, use or disclosure of personal information; an information security incident is a threat to the secure and effective operations of our network or IT infrastructure. We have a detailed incident response protocol that ensures rapid containment and analysis of an incident, appropriate notification to clients and affected individuals, risk mitigation measures where personal information has been compromised, and compliance with any legal obligations that may arise as a result of the incident. In the wake of any privacy or security incident, we will conduct and document a full evaluation of the causes and contributing factors and implement appropriate changes to systems and processes to avoid a reoccurrence.

Sterling Volunteers

Legal Compliance

Sterling Volunteers' systems, policies and procedures are designed to meet or exceed all requirements set out in data protection, privacy and consumer reporting laws in all jurisdictions in which we operate. Some examples include:

United States

- Federal Fair Credit Reporting Act [15 U.S.C. § 1681]
- California Credit Reporting Agencies Act [Civil Code §1785.1 et seq.]
- Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth [201 CMR 17.00]

Canada

- Federal Personal Information Protection and Electronic Documents Act
- Quebec Act Respecting the Protection of Personal Information in the Private Sector
- Alberta Personal Information Protection Act
- British Columbia Personal Information Protection Act
- Ontario Freedom of Information and Protection of Privacy Act
- British Columbia Business Practices and Consumer Protection Act

European Union

- EU Data Protection Directive 95/46/EC
- United Kingdom: Data Protection Act 1998
- Germany: Bundesdatenschutzgesetz
- France: Loi informatique et libertés
- EU ePrivacy Directive 2002/58/EC

World-Class Protection for International Reach

In order to maintain the global reach and deliver the quality and breadth of service that our customers expect, Sterling Volunteers employs operational resources that cover 200 countries, territories, and dependencies. Sterling Volunteers complies with all national and local laws and regulations with respect to the storage and transmission of sensitive data and personal information. During the normal course of our business, data is hosted in secure data centers in the United States. This data is accessed by Sterling Volunteers employees located in the United States, the Philippines and India, countries specifically chosen to optimize efficiency, quality, and cost for our customers. This globally diverse presence allows Sterling Volunteers to provide the world class service that our customers have come to expect.

Sterling Volunteers' operational resources access data stored on secured servers located inside the United States from our facilities around the world. Access is restricted to only that data which is needed to fulfill the request, and is encrypted while it is being transmitted. In addition, access is restricted to devices that do not allow the download of data to removable media or storage on any system. Data is displayed to the user using secure virtualization technology and is not downloaded or stored on local devices. Operational facilities are secured locations, and all employees are fully screened by Sterling Volunteers. Operational facilities enforce clean desk policies, restricted printing, and no recording devices to help ensure that data remains secure. Sterling Volunteers further enhances the security of our systems by ensuring all outbound e-mail is screened for sensitive data and encrypts that data before it is transmitted. Regardless of the location from which the work is performed, the same information security standards and technologies are applied, ensuring uniform security and operational excellence from every facility. Sterling Volunteers has various mechanisms in place to help its customers ensure that international data transfers are compliant with restrictions imposed by applicable data protection and privacy laws around the world, such as templates for EU Standard Contractual Clauses and sample multilingual privacy notices.