SGI ISMS INFORMATION SECURITY POLICY

ISO 27001 ISMS Policies & Procedures

Abstract

This standard ensures that SGI complies with the ISO 27001 security principles

Information Security Policy

Policy Overview

This policy is based on ISO 27001, the recognized international standard for information security. This standard ensures that the organization follows the following security principles:

- Confidentiality: sensitive information will be protected from unauthorized access or disclosure; and
- Integrity: information will be protected from accidental, malicious, and fraudulent alteration or destruction; and
- Availability: Information services will be available throughout the times agreed with the users and will be protected against accidental or malicious damage or denial of service.

SGI is committed to ensuring that all these aspects of information security are followed to fulfill its statutory functions.

The President approves this policy. The Security Officer has the responsibility for ensuring that the policy is implemented and adhered to.

The security policy confirms SGI's commitment to continuous improvement and highlights the key areas to effectively secure its information.

Policy Detail

Senior Management Responsibilities and Commitments

Senior management is committed to satisfying all applicable requirements within this policy and to the continual improvement of the Information Security Management System (ISMS), and therefore have set up this information security policy so that:

- It is proper to the purpose of the organization.
- It includes information security objectives and provides the framework for setting continual information security objectives.

This information security policy shall be available as documented information; be communicated within the organization and be available to interested parties, as appropriate.

Leadership and commitment

Senior management will continue to show leadership and commitment with respect to the information security management system by:

- Ensuring the information security policy and information security objectives are established and are compatible with the strategic business direction of the organization.
- Ensuring the integration of the information security management system requirements into the organization's processes.

- Ensuring that the resources needed for the information security management system are available.
- Communicating the importance of effective information security management and of conforming to the information security management system requirements
- Ensuring that the information security management system achieves its intended outcomes(s)
- Directing and supporting people to contribute to the effectiveness of the information security management system.
- Promoting continual improvement and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

Information Security Objectives

Information security objectives have been established and are compatible with the strategic direction of the organization, the key objective is to work in line with the sections of the best practice standard ISO 27001 detailed below.

Furthermore, security objectives will be set by management as an ongoing task and at ISMS Management Review Meetings information security objectives will be produced and implemented as part of the ISMS.

Management Objectives for information security will be continually set and monitored to ensure they are achieved.

SGI will look to continually improve the information security management system in line with a Plan-Do-Check-Act method to improve processes embedded within its ISMS.

Organization of Information Security

The importance attached to information security within SGI is demonstrated by the participation of senior management; the role of senior management is outlined below:

- Reviewing and progressing strategic security issues
- Establishing relationships outside of SGI with other security advisers
- Assessing the impact of new statutory or regulatory requirements imposed on SGI.
- Monitoring the effectiveness of the Information Security Management System (ISMS) from results of Internal Audit Reports and External Security Audits.

Senior management meets regularly to address the above activities to ensure the continuing effectiveness of SGI’s ISMS. The review process is defined in the ISMS Management Review Policy.

Classification of Information

SGI is an agile dynamic organization with limited resources for managing overly complex marking schemes. It does, however, recognize the importance of effective information classification to protect information and assets based on its value, importance or associated legal liabilities if managed incorrectly.

The organization is prevented from profiting from the client and patient data we manage outside of payment for our services under contractual agreements with our clients. In other words, SGI is prohibited from selling or distributing data used to support our clients and must make all reasonable efforts to avoid unintentional or malicious distribution of this data outside of its intended use.

To that end, Information that is accessible from the SGI systems is classified as follows:

"Public"

The information can be shared widely with no limitations on use because it is neither covered under confidentiality clauses in contracts or legal liability (HIPAA violation, Identity Theft, etc.).

"Confidential"

Non-sensitive information, whether provided by the client or gathered while fulfilling service requests for the client, that if disclosed would violate a confidentiality clause within an existing contract falls into this category.

Information is available on a “need to know” basis relative to the role being performed by the individual within a department.

Source code for our applications falls into this category. Though the loss would be significant the ability for others to replicate and use the source code is highly limited.

Personal Identifiable Information (PII) that is not covered under HIPAA falls into this category. Examples are individual orders placed for shipment of material. These orders are placed by client employees, who are authorized to do such. Recipients are typically themselves or health care providers. Direct shipments to patients from our client employees are restricted under HIPAA. The extent of the PII information involved is only what is necessary to ship them the requested order.

"Sensitive"

For information where unintended or unauthorized disclosure or loss has a serious impact on strategic objectives or puts the survival of the organization at risk.

HIPAA related patient data falls into this category due to the legal and contractual violations that could ensue should unintended or malicious disclosure occur.

Employee data that could lead to identity theft leading to legal liabilities fall into this category.

Access credentials such as passwords, datacenter card access, administrative rights, etc. are considered sensitive due to the potential risks of access to systems containing sensitive data.

Information is available on a “need to know” basis relative to the role being performed by the individual within a department.

Compliance with SGI’s security policies and procedures is mandatory for all personnel.

Human Resource Security

All employees must sign the SGI Employee Handbook which requires them to work in accordance with all policies and procedures, which includes information security specific requirements. Furthermore, an Acceptable Usage Policy ensures that employees are made aware that they are required to follow best practices regarding information security established by SGI. There are procedures for all employees that leave SGI (including temporary and contract employees) to disable their network account and recover all items of property.

All new employees must be trained on procedures in the areas described above as part of their induction program.

Mobile Device and Teleworking

SGI supports the ability for approved employees to service our clients remotely using approved devices and methods outlined in our ISMS. When working remotely from SGI's facilities users must adhere to the Acceptable Usage Policy and guidance contained therein when it comes to using public Wi-Fi networks, for example. Users are responsible to ensure that when connecting to the internet they are doing so in a safe and secure manner in compliance with our ISMS.

Asset Management

SGI information must be classified according to its sensitivity and an information owner assigned. The IT Team will maintain an information asset inventory which is updated periodically, according to its risk profile and protected accordingly.

Access Control

Employees must be aware of and must follow controls and procedures which exist to limit access to confidential information. The IT Team are responsible for both establishing and maintaining robust logical access controls.

Cryptography

Where SGI employs cryptographic controls a policy on the use of cryptographic controls for protection of information must be developed and implemented.

Physical and Environmental Security

Staff must be aware of and must follow the detailed set of measures, controls and procedures that exist to ensure adequate control of physical security. They include:

- Building and individual alarm systems
- Restricted access to the building and further restricted access within it
- Secure offsite backups and archiving

Operations Security

SGI will ensure correct and secure operations of information processing facilities.

Communications Security

Staff must be aware that the use of technology and communications are established, controlled, and managed by the IT Team. The IT department is responsible for ensuring that the appropriate security measures and processes are in place. SGI will ensure that security around the network, mobile and remote working are adequately protected.

System Acquisition, Development and Maintenance

SGI must ensure that the appropriate information security processes are included in all projects that acquire, develop or maintain software used in the conduct of its business.

Supplier Relationships

Information security requirements for mitigating the risks associated with supplier’s access to the organization’s assets must be agreed with the supplier and documented.

Information Security Incident Management

Security incident management records must be centrally maintained, updated, and monitored. All employees must be aware of what constitutes an actual or potential security incident, how to report the incident and who to report the incident to.

A security incident is any event resulting from malicious intent that compromise the:

- confidentiality of sensitive information
- integrity of information critical to the support of our business
- loss of access to information critical to the support of our business

Security incidents are to be reported immediately to the Security Officer when they are discovered.

The responsibility for the oversight of incidents rests with the Security Officer.

Information Security Aspects of Business Continuity Management

The organization must ensure a consistent and effective approach to the management of major information security incidents, including communication on security events and weaknesses and the implications for business continuity management.

Compliance

SGI must avoid security incidents of legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements.

SGI must take technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss or alteration, and unauthorized disclosure or access. SGI takes measures that are intended to ensure that:

- Anyone managing sensitive data understands that they are contractually responsible for following good data protection practices.
- Everyone managing sensitive data is appropriately trained to do so.
- Everyone managing sensitive data is appropriately supervised.

Review

This document must be reviewed at least annually by SGI’s President. The Security Officer must ensure the correct version number is applied to the document once the review has taken place.

Enforcement

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

Compliance

The document owner or a nominated proxy will conduct regular compliance review of this document and record evidence of the review, along with any corrective or preventative actions that have been agreed because of non-compliance occurrences.

Signed

Jack K. Burns

Jack K. Burns
President SGI

Version	Date	Responsable Person	Description of Change
1	11/08/2021	Forrest Adam	Initial Release ISO 27001:2013
2	12/10/2021	Forrest Adam	Updated to reflect comments from our ISO gap auditor