Client operations & Insights

Information Security Policy

Purpose

Settlement Services International Limited and its subsidiary entities (SSI Group) is committed to managing information security in accordance with the organizational policies, and relevant contractual requirements, laws and regulations.

The purpose of this policy is to outline how SSI Group manages and mitigates security risks to safeguard the confidentiality, integrity, and availability of SSI Group information, technology assets and business environment.

Scope

This policy applies to all Board members, employees, volunteers, contractors, entrusted third party service providers and other members of the supply chain who are provided access to SSI Group's systems or data in the delivery of their services.

It is the responsibility of each person in scope to ensure compliance with this policy.

Policy Statement

SSI Group is committed to the secure management of information and systems utilising a policy framework based on the international standard for security management systems – ISO 27001. SSI Group manages information security risks and controls to the extent that there are clear benefits and applicable to the organisation.

Information Security Principles

SSI Group has adopted the following high-level Information security principles to establish a sound foundation for information security policies, procedures and practices.

- Information, in whatever form (including paper based), is managed utilising a framework based on international standard ISO 27001.

- SSI Group only collects, holds, uses, and discloses personal and health information of client, customer, employee or another person (such as contractor) for the purpose of carrying out its functions.

- Information security risks are managed considering broader SSI Group's information security objectives, strategies and priorities.

- SSI Group management actively promotes an organisational culture that supports information security management through clear direction, demonstrated commitment, and explicit assignment of information security responsibilities.

- Secure access use and disposal of information technology platforms and data is managed as per the guidance provided in ITC policy.

- Information security incidents are managed effectively as per the documented incident response plan.

- Management of any adverse event and recovery of critical business functions is carried out as per the documented Business Continuity Plan.

Responsibilities

Board of Directors – SSI Group Board assume oversight responsibility in managing information security risks.

CEO and General Managers – Operational responsibility for information security rests with the SSI Group's CEO, however responsibilities for the management of information security within specific program/function is also delegated to the respective general managers.

Information Security Officer (ISO) – Responsible for aligning business and security objectives with contractual requirements, providing strategic security direction to ensuring compliance with policy, standards, regulations and legislation.

Site Managers – Responsible for the day-to-day physical protective security measures at the site.

Employees, Contractors and Volunteers – All staff members must adhere to their obligations in relation to the information security policy and associated procedures and guidelines. They are also responsible for reporting any suspected or actual security breaches.

Maintenance

SSI Group maintains a suite of relevant security-related policies and procedures. Updates to key policies and procedures are performed every 12 months or as deemed appropriate based on changes in technology or regulatory requirements.

Enforcement

Violations of this Policy may result in suspension or loss of the violator's use privileges, with respect to SSI Group's data and information systems. Non-compliance with the policy will be dealt with by appropriate measures ranging from disciplinary to legal action.

Exceptions to this Policy must be approved by the General Manager of respective business division and formally documented. Policy exceptions will be reviewed by Information Security Officer on a periodic basis for appropriateness.

Definitions

Term	Definition
Digital Data	Nontangible information assets
ICT asset	Any hardware or data used for or related to information technology or communication.
Information	Any data (both structured and unstructured), irrespective of its file format and/or its storage medium.
Information asset	Any information that is of value to the organisation. This term also includes the underlying supporting infrastructure such as business processes, hardware, networks, storage, applications, and third-party providers amongst others.
Information security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
IT Infrastructure	For the purposes of this policy, the term “IT infrastructure” applies to (but is not limited to) the following Infrastructure components owned by, leased to, and/or managed on behalf of SSI Group: - Networks - Server systems - Personal computing devices - laptops, desktops, mobile devices including smart phones - Gateways, firewalls, and other network perimeter security devices - System software - Operations components – monitoring/managing
Physical assets	Tangible information assets (paper documents, backup tapes etc.)