ISMS-ISG-005-Information Security Policy and Objectives

Information Services Group, Inc

Owner:	Ankith C K
Version:	2.5
Date:	14 Jul 2025

Document Control

Date/Reviewer	Details of Change	Revision Made By
27 April 2016	Draft document	Julian Bower
19 Aug 2016	First complete draft	Julian Bower
11 Nov 2016	Updated section 2.1, following Stage 1 audit	Julian Bower
06 Sept 2018	Annual review	Julian Bower
09 Oct 2019	Annual review	Julian Bower
28th May 2020	Updated the InfoSec Objectives	Sweety Motwani
14th Oct 2020	Annual review	Julian Bower
15th Jul 2021	1.6 Updated the InfoSec Objectives	Sweety Motwani
29th Oct 2021	1.7 Annual review	Sweety Motwani
9th June 2022/Julian Bower	1.8 Merged the contents of India ISMS into this document	Sweety Motwani
1st Dec 2022/ Julian Bower	1.9 Periodic Review	Ankith C.K.
6th Jun 2023/David Hull	2.0 - Changed the Owner from Julian Bower to David Hull	Sweety Motwani
21st Sept 2023	Annual Review - v2.1	David Hull
1st August 2024	2.2 - Updated the ISO27001 Control References from 2022 Version	Sweety Motwani
11 Feb 2025	2.3 - Added Section 2.12	Ankith C K
13 May 2025	2.4 – Added Approval History	Ankith C K
08 Jul 2025	2.5 – Changed owner details. Updated section 2.4.2	Ankith C K, Julia Allison

Approval History

Date	Details of Change	Approved by
13th May 2025	Changes approved (v2.4)	David Hull
14th Jul 2025	Changes Approved (v2.5)	David Hull

Access List

List of Users	Access Type	Type of Media	Retention Period
Information Security Management Team	Read/Write/Delete	Soft Copy	Default
Information Security Team	Read/Write	Soft Copy	Default
ISG employees	Read	Soft Copy	Default

Table of Contents

1 Policy Control

1.1 Introduction

This policy outlines the Information Security objectives of Information Services Group, Inc, our commitment as an organization to satisfy all applicable Information Security requirements and the ongoing improvement of the Information Security Management System. It also summarizes the key policy documents that are in operation and management of the Information Security Management System.

1.2 Notice of Compliance

Security is the responsibility of everyone affiliated with Information Services Group, Inc referred to as ISG henceforth, or directly accessing ISG systems, ISG data, and data entrusted to ISG by clients or other third parties. The security measures described herein define the basic minimum level of security required for ISG systems and information. Non-compliance with the required security measures and behaviors outlined in this policy could pose significant business and legal risk to ISG, and may create a potential for legal actions that could significantly impact ISG's operations and damage its business assets and reputation. Such action may include, but is not limited to, reprimand, financial penalties, termination of employment, and/or legal action. Therefore, compliance with this policy and all ISG security-related policies, are mandatory conditions for employment for all ISG people, as well as any third parties (such as outsourcing providers, contractors, alliance partners, clients, etc.) that access ISG systems or data. No one is permitted to bypass the security mechanisms provided by ISG systems or infrastructure for any reason.

1.3 Exception, Migration and Time Frames

All ISG employees, contractors and systems must comply with the statements in this policy with immediate effect.

Where a longer transition is required to achieve compliance, a documented business justification must be submitted with proposed timelines as a Security Exception to the Information Security Management Team for approval.

Any exceptions to this Policy must be clearly documented and submitted to the Information Security Management team for evaluation and approval. Only exceptions which have been approved are valid.

1.4 Contact Information

For any questions regarding this policy, please contact

Group	Information Security Management Team
Email	**isgsecurity@isg-one.com**

2 Information Security Policy

2.1 Policy

ISG shall endeavor to ensure that the information and the information processing facilities are protected and made secure from all known security threats arising both internally and externally.

ISG shall strive to secure information by:

- Establishing and maintaining an effective Information Security Management System (ISMS);
- Performing risk assessment periodically;
- Implementing information security controls to mitigate the identified risks;
- Complying with legal, regulatory and contractual information security requirements;
- Establishing an effective Business Continuity Management Framework;
- Deploying the most appropriate technology and infrastructure;
- Creating a security conscious culture;
- Continually monitoring and improving the effectiveness of the ISMS.
- Comply with the Information Security Objectives, listed below

2.2 Information Security Objectives:

- To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
- To implement the necessary security controls for all the identified risks and lower the risk exposure to an acceptable level.
- To ensure that employees and contractors are aware of and fulfil their information security responsibilities.
- To protect the organization’s business information and any client or customer information within its custody or safekeeping by safeguarding its confidentiality, integrity and availability.
- To ensure all information security incidents are recorded and addressed with appropriate Corrective and Preventive actions.
- To ensure that information security is designed and implemented within the standard operations of information systems.

2.3 Information Security Requirements

ISG, in its requirements for information security, shall include but not limit itself to, the following:

- Requirements arising from assessment of risks
- Legal, statutory, regulatory and contractual requirements
- Any changes in organization or business strategy that may affect Information Security

2.4 Compliance with the Information Security Management System

All ISG employees, contractors and third-parties shall be compliant with the ISMS and any violation may lead to disciplinary action triggering the section 5.11 of the "HR Security Procedure"

In this section we highlight our policies that are of material relevance for all

2.4.1 Technology Acceptable Use Policy

The Technology Acceptable Use Policy is published on the Information Security site on OneX. It outlines detailed instructions on how ISG's IT equipment and systems are to be used and is to be read and complied with by all ISG personnel, including permanent members of staff, contract, and temporary appointees.

2.4.2 Data Protection and Privacy Policy

The Employee (and Contractor) Data Protection and Privacy policy is published in the "People" Global Policies and Procedures section on OneX. The principal laws that apply to ISG's locations are:

- UK - The Data Protection Act 2018 ("DPA 2018"). The DPA 2018 implements EC Council Directive 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Germany - The Federal Data Protection Act 2017 (BDSG)
- Italy – The Privacy Code was harmonized with the GDPR in 2018
- All other EU countries - The General Data Protection Regulation (EC Council Directive 2016/679)
- India – The Digital Personal Data Protection Action 2023

- Canada – The Personal Information Protection and Electronic Documents Act (PIPEDA).
- US – Various US State Privacy Laws (see ISMS-ISG-018 Compliance Procedure for full list)

Breach of the Personal Data Protection (PDP) laws may severely impact ISG's business. Data Protection Authorities have extensive powers when monitoring the application of regulations, in order to protect the fundamental rights and freedoms of data subjects. The following Data Protection Authorities are relevant for ISG locations:

- UK – ICO
- Germany - Der Hessische Beauftragte fur Datenschutz and Informationafreiheit
- Italy – Garante per la Protezione De Dati Personali (GPDP)
- France - Commission National de l'Informatique et des Libertes (CNIL)
- Australia - Office of the Australian Information Commissioner
- India – Awaiting confirmation of the independent authority following on from the enactment of DPDP Act 2023
- US - There is no single national authority. Consider state by state.

ISG takes compliance with PDP laws very seriously. ISG employees must ensure they are operating in line with our policy and receive annual formal data protection and privacy training and periodic awareness reminders.

2.5 Review of the Information Security Policy

The Information Security Policy shall be reviewed annually and as and when significant changes occur, by the Information Security Committee (ISC) to ensure its continuing relevance and accuracy.

2.6 Management of the ISMS

The ISC shall regularly convene to review the effectiveness of the ISMS implemented within the organization and shall act as the final approving authority for all information security-related decisions, ISMS documentation and any subsequent changes made.

The ISC shall allocate information security responsibilities to appropriate personnel.

2.7 Employee Confidentiality Agreements

The ISC shall identify and review the requirements for the protection of information among employees and work with HR (who manage the process) to maintain confidentiality agreements signed by all employees and third-party staff.

2.8 Contact with Authorities and Special Interest Groups

ISG shall maintain up-to-date contact details of the relevant civil authorities including but not limited to medical services, police stations, and the fire brigade that are to be contacted during a crisis.

ISG shall also maintain professional associations with special interest groups in the area of information security to be abreast of the information security best practices.

2.9 Independent Review of Information Security

ISG shall ensure that the organization's approach to managing information security, and its implementation are reviewed independently at regular intervals, or when significant changes occur with minimal risk of disruptions to business processes.

2.10 Addressing Security with External Parties

ISG shall cover all relevant security requirements while entering into an agreement with external parties involving accessing, processing, communicating or managing the organization's information or information processing facilities.

2.11 Third Party Service Delivery Management

ISG shall ensure that the security controls, service definitions and delivery levels mentioned in the agreement with the third party service provider shall be implemented, operated and maintained by the third party.

ISG shall, on a regular basis, monitor the service levels and quality of the third party service provider through means such as review of service reports.

ISG shall manage the changes to the terms of the third party service provider agreements considering the criticality of the business systems or processes involved and re-assessment of risks.

2.12 Continual Improvement

ISG is committed to the continual improvement of Information Security Management System (ISMS) to ensure the confidentiality, integrity, and availability of all sensitive information handled.

To achieve continual improvement, the following are performed [not limited to]:

1. **Regularly Review and Assess Security Risks**
2. **Implement Corrective and Preventive Actions as necessary**
3. **Monitor Performance and Effectiveness**
4. **Ongoing Training and Awareness Programs**
5. **Feedback and Collaboration**.

ISG ensures that its ISMS remains adaptable, resilient, and aligned with the best practices, thus protecting the interests of clients, stakeholders, and employees.

3 ISO 27001 References

2013 Version:

- A.5.1.1 Policies for Information Security
- A.5.1.2 Review of the policies for information security
- A.6.1.1 Information security roles and responsibilities
- A.6.1.2 Segregation of duties
- A.6.1.3 Contact with Authorities
- A.6.1.4 Contact with Special interest groups
- A.6.1.5 Information security in project management
- A.12.7.1 Information systems audit controls
- A.13.2.4 Confidentiality or non-disclosure agreement
- A.18.2.1 Independent review of information security
- A.15.1.1 Information security policy for supplier relationships
- A.15.1.2 Addressing security within supplier agreements
- A.15.1.3 Information and communication technology supply chain
- A.15.2.1 Monitoring and review of supplier services
- A.15.2.2 Managing changes to third party services

2022 Version:

- 5.1 Policies for Information Security, Review of the policies for information security
- 5.2 Information security roles and responsibilities
- 5.3 Segregation of duties
- 5.5 Contact with Authorities
- 5.6 Contact with Special interest groups
- 5.8 Information security in project management
- 8.34 Information systems audit controls
- 6.6 Confidentiality or non-disclosure agreement
- 5.31 Independent review of information security
- 5.19 Information security policy for supplier relationships
- 5.20 Addressing security within supplier agreements, Information and communication technology supply chain
- 5.22 Monitoring and review of supplier services, Managing changes to third party services

4 Glossary of Terms

1. **Asset**

Anything that has value to the organization

2. **Control**

Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature

3. **Guideline**

A description that clarifies what should be done and how, to achieve the objectives set out in policies

4. **Information Processing Facilities**

Any information processing system, service or infrastructure, or the physical locations housing them

5. **Information Security**

Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non – repudiation, and reliability can also be involved

6. **Information Security Event**

An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

7. **Information Security Incident**

An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

8. **Policy**

Overall intention and direction as formally expressed by management

9. **Risk**

Combination of probability of occurrence of an event and its consequence

10. **Risk Analysis**

Systematic use of information to identify sources and to estimate the risk

11. **Risk Assessment**

Overall process of risk analysis and risk evaluation

12. **Risk Evaluation**

Process of comparing the estimated risk against given risk criteria to determine the significance of the risk

13. **Risk Management**

Coordinated activities to direct and control an organization with regard to risk

14. **Risk Treatment**

Process of selection and implementation of measures to modify risk

15. **Third Party**

That person or body that is recognized as being independent of the parties involved, as concerns the issue in question

16. **Threat**

A potential cause of an unwanted incident, which may result in harm to the organization

17. **Vulnerability**

A weakness of an asset or a group of assets that can be exploited by one or more threats