SC&H Group ISMS Policy [Public]

Table of Contents

1. Policy

The purpose of the SC&H Group, Inc. "Information Security Management System" policy (the "Policy") is to describe the Information Security Management System (ISMS) adopted for SC&H Group, Inc. for all systems which store or provide access to sensitive customer information with emphasis on accomplishing the ISMS policy and objectives. The section contents of the policy are aligned with ISO 27001:2022 for easy reference.

This Policy applies to all SC&H Group, Inc. employees, affiliates and all other individuals or companies such as external partners or suppliers who have access to, or are responsible for, SC&H Group, Inc. information regardless of its form or medium. This Policy applies to all SC&H Group, Inc. personal and sensitive data (e.g. candidate, client, and employee data collected in electronic or hard copy form that is generated, maintained, and entrusted to SC&H Group, Inc. except where a different standard is required by contract, or by law. This Policy is effective immediately and may be changed at any time.

In addition, this policy also applies to all employees, management, contractors, vendors, business partners, and any other parties who have access to company data.

2. Acronyms & Definitions

2.1 Acronyms

IRP	Incident Response Plan
ISMS	Information Security Management System
ISSA	Information Systems Security Association
SIRT	Security Incident Response Team
SOP	Standard Operating Procedure

2.2 Definitions

Asset	Something, which is of value to the organization, its business operations and their continuity and needs to be protected
Assurance	The confidence that may be held in the security provided by a system, product or process
Availability	Ensuring that authorized users have access to information and associated assets when required
Configuration Control	A system of controls imposed on changing controlled objects including documentation
Evaluation	The assessment of an IT system or product against defined criteria
Firewall	Data communications barrier that is trusted to limit the data that passes across it by implementation of network access control rules.
Impact	The result of an unwanted incident
Information Assets	Databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, etc.

Information Security	Security preservation of confidentiality, integrity and availability
Information Security Management System (ISMS)	That part of the overall management system, based on a business risk approach that establishes, implements, operates, monitors, reviews, maintains and improves information security
Information Security Policy	The set of laws, rules and practices that regulate how assets, including sensitive information, are managed, protected and distributed
Integrity	Safeguarding the accuracy and completeness of information and processing methods
The Company Information Assets	The Company Information Assets means all data of any kind regardless of ownership, touching The Company Systems. This includes client data, emails, and other digital communications; intellectual property; strategic, operational, business, and marketing plans; engineering ideas and designs; research and reports; software code; compensation information and all unpublished financial data of the Company.

4. Information Security Management System

4.1 Context To The Organization

The Company has identified, developed and implemented a means to identify information security issues as they relate to security demands. The following high-level issues have been identified:

- Customer Regulatory, Compliance and Contractual Obligations
- Prevent and detect cyber attacks
- Mature capabilities of information security program
- Address board of director and senior leadership agenda
- Comply with relevant regulations and standards:
  - GDPR (EU)
  - Microsoft SSPA
  - California Privacy Rights Act (California)
  - Consumer Data Protection Act (Virginia)
  - Colorado Privacy Act

As issues are identified, their part in the overall ISMS plan will be determined and documented. Risks, when appropriate, will be identified and treated.

4.2 Needs and Expectations of Interested Parties

Office of the Chief Information Officer (CIO) is responsible for identifying and maintaining all internal and external parties that may affect the ISMS, along with the requirements of these parties. The following table defines the parties and requirements.

Internal Parties

Role	Objectives/Requirements
Chief Information Officer (CIO)	▪ Mitigating and reducing data privacy risk and liability ▪ Positioning the company and products as being secure ▪ Information security policies ▪ Objectives for the SC&H Group, Inc. ISMS ▪ Management review ▪ Maintaining GDPR compliance
Virtual Chief Information Security Officer (vCISO)	▪ Mitigating and reducing information security risk and liability ▪ Positioning the company and products as being secure ▪ Internal audit ▪ Information security policies ▪ Objectives for the SC&H Group's ISMS ▪ Management review ▪ Management aspects of business continuity and disaster recovery
Global Data Privacy Officer (DPO)	▪ Mitigating and reducing data privacy risk and liability ▪ Positioning the company and products as being secure ▪ Information security policies ▪ Objectives for the SC&H Group's ISMS ▪ Management review ▪ Maintaining GDPR compliance
SC&H Group, Information Technology	▪ System acquisition, development and maintenance ▪ Operational aspects of access controls ▪ Asset management ▪ Responsibility for implementing information security risk treatment ▪ plans ▪ Operational aspect of business continuity and disaster recovery
SC&H Group, Information Security and Privacy Committee	▪ Information Security Operations & Engineering ▪ Information security incident management ▪ Access Controls ▪ Cryptography ▪ Education, training and awareness ▪ IT Risk Management (includes privacy risks) ▪ Privacy considerations ▪ Personal information identification
General Employees	▪ Use company data responsibly ▪ Comply with company policies ▪ Report suspicious activity
Human Resources	▪ Human resources policies ▪ Recruiting and screening ▪ Ensuring competency
Customer Service	▪ Securely accessing PHI and PII ▪ Secure disposal of hard copy PHI and PII
Corporate Security	▪ Physical and environmental security of corporate offices

External Parties

Role	Objectives/Requirements
Microsoft Azure	Microsoft is required to maintain their ISO 27001 certifications. Microsoft is also required to maintain physical security and environmental requirements. SC&H Group, Inc. is required to design and maintain secure engineering principles within the Microsoft Virtual Networks.
Clients	SC&H Group, Inc. clients require that their PII is managed securely. Clients require that SC&H Group, Inc. does not share or expose their customer information outside of contracted agreements.
Data Subjects	Consent to data collection. Provide accurate data (when applicable).
Governing Bodies	Set regulations for protecting certain data types and requiring specified reporting of incidents. GDPR/EU Privacy Counsel. California Consumer Privacy Act (CCPA).
Security Consultant (vCISO)	Advise the organization of security best practices, risks, and serve as a trusted consultant.
Security Operations Center (MSSP)	The vendor is responsible for monitoring the SIEM and escalating any suspicious activity to SC&H Group, Inc. SC&H Group, Inc. is responsible for receiving alerts, investigating and responding appropriately.
Outsourced Web Hosting	Outsourced Web Hosts are required to meet SC&H Group, Inc. ISMS security requirements. SC&H Group, Inc. is responsible for supervising and monitoring. Additionally, they are responsible for following SC&H Group, Inc.'s Privacy by Design Process.
Legal Counsel	Provide advice on relevant regulatory compliance that the company must adhere to. In the event of material incident or breach, provide counsel to best abide by regulatory compliance reporting mandates.

4.3 Scope of the ISMS

SC&H Group's Information Security Management System (ISMS) covers the security and privacy of candidate, client, participant and employee personal data within the following groups of products or services: organizational strategy, assessment & succession, talent acquisition, leadership, and development. This is in accordance with the Statement of Applicability (SOA) v1.0 dated February 21, 2025.

SC&H has defined and developed the scope of the Information Security and Privacy Management System (ISPMS) according to the requirements outlined in Clause 4.3 of the ISO 27001:2022 and ISO 27701:2019 standards. The established scope statement is:

The SC&H Information Security Management System (ISMS) and Privacy Management System (ISPMS) scope applies to the company's infrastructure, operations, security, and delivery of the following services:

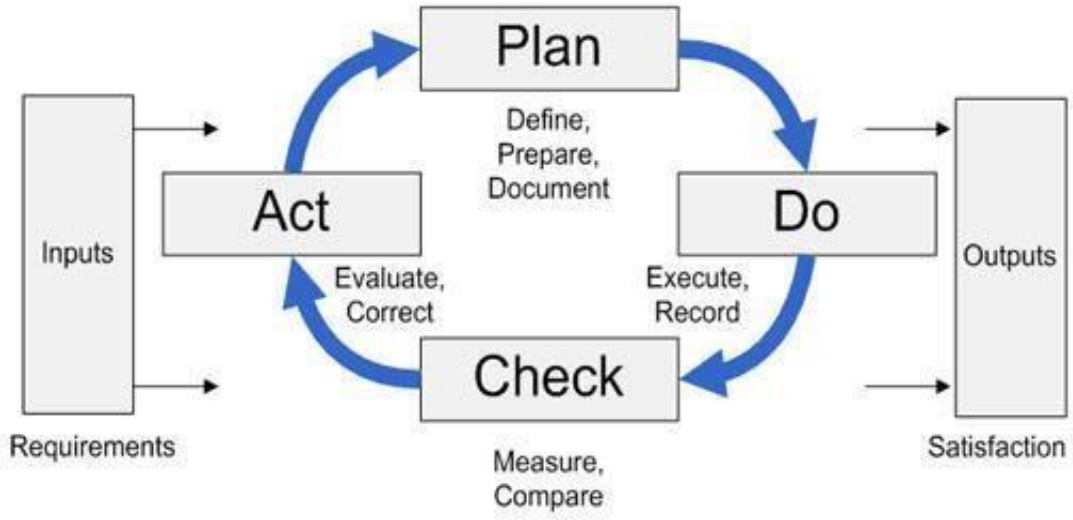
- Advisory & Transformation
- Technology
- Risk
- Accounting
- Audit
- Tax
- Capital
- Wealth

Locations:

- Sparks Glencoe, MD - (HQ)

4.4 Information Security Management System

SC&H Group has developed, implemented, maintained and continually improved the documented ISMS within the context of the organization's overall business activities and risk. The standard process used is based on the Plan, Do, Check, Act (PDCA) model given below:



The way SC&H Group applies the PDCA model is documented throughout the remaining sections of this policy.

5. Leadership

5.1 Leadership and Commitment

Breach of Information Security Policies

Policy Ownership and Maintenance

5.2 Policy

5.3 Roles & Responsibilities

SC&H Group Information Security and Privacy Committee (Privacy and Security Management)

SC&H Group Information Security and Privacy Committee (Security Operations)
SC&H Group Infrastructure Operations

Internal and External Parties

6. Planning

6.1.1 Actions to Address Risks and Opportunities

6.1.2 Security and Privacy Risk Assessment

6.1.3 Security and Privacy Risk Treatment and Controls

6.2 Security and Privacy Objectives and Planning to Achieve Them

6.3 Planning of Changes

7. Support

7.1 Resources
7.2 Competence
7.3 Awareness
7.4 Communication

7.5 Documented Information

7.5.1 General
7.5.2 Creating and Updating

7.5.3 Control of Documents
8. Operation

8.1 Operational Planning and Control
8.2 Risk Assessment
8.3 Risk Treatment
9. Performance Evaluation

9.1 Monitoring, Measurement, Analysis and Evaluation
9.2 Internal Audit
9.3 Management Review

10. Improvement

10.1 Nonconformity and Corrective Action

10.2 Continuous Improvement
11. Compliance

12. Revision History

Version	Date of Change	Approved By	Revision Summary
1.0	06/01/2024	Zach Kehring, CIO	Initial Policy
2.0	03/07/2025	Zach Kehring, CIO	Organization