Information Security Management System

Policy Statement

SC&H Group, Inc. • schgroup.com

Purpose

SC&H Group, Inc. ("SC&H") has established and maintains a formal Information Security Management System (ISMS) to protect the confidentiality, integrity, and availability of information assets entrusted to the organization by its clients, employees, and partners.

This Policy Statement describes SC&H's commitment to information security and summarizes the principles governing our ISMS. The full ISMS is maintained internally and is aligned with the ISO 27001:2022 standard.

Scope

The SC&H ISMS applies to the company's infrastructure, operations, security practices, and delivery of the following services:

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

This policy applies to all SC&H personnel, including employees, contractors, temporary staff, and third parties who access SC&H systems or handle SC&H information in any form.

Our Security Commitments

SC&H is committed to maintaining and continually improving information security to minimize risk exposure and ensure business continuity. Specifically, we are committed to:

> **Confidentiality** Information is accessible only to those authorized for access.
>
> **Integrity** Information is accurate, complete, and protected from unauthorized modification.
>
> **Availability** Authorized users and systems can access information when required.

ISO 27001:2022 Alignment

SC&H's ISMS is structured in alignment with the ISO 27001:2022 standard, employing a Plan–Do–Check–Act (PDCA) model for continuous improvement. Our program includes:

- Annual security risk assessments and formal risk treatment plans
- Defined roles and responsibilities for information security governance
- Security awareness training required for all personnel on an annual basis
- Formal incident response procedures
- Regular internal audits and management reviews
- Documented policies governing access control, cryptography, physical security, and operational procedures

Responsibilities

All individuals with access to SC&H systems and information assets are required to understand and comply with this policy and all supporting information security policies. Violations may result in disciplinary action, loss of access privileges, or legal action, including termination of employment or referral for criminal prosecution.

SC&H retains the right to revoke access to systems at any time, with or without cause, at its sole discretion.

Reporting Security Concerns

Any employee, contractor, or third party who becomes aware of a suspected or actual security incident, unauthorized access, or policy violation is required to report it promptly to the SC&H IT Department at helpdesk@schgroup.com or directly to the Chief Information Officer.

Policy Governance

This Policy Statement is owned and maintained by the Office of the Chief Information Officer (CIO). It is reviewed and updated at least annually, or upon significant changes to SC&H's operational or regulatory environment.

SC&H's complete suite of internal information security policies is available to employees, auditors, and relevant external parties upon request and as appropriate to their role and relationship with SC&H.

Effective Date: March 20, 2026 · **Version:** 5.0 · **Approved by:** Office of the Chief Information Officer