INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

Document History

Document Owner:	CEO
Document Number:	SCP-P-070
Revision Number:	11.0
Issue Date:	28TH June 2023

This is a controlled document, please ensure that this document is the most recent version by checking on SharePoint. If you require a change to this policy, please contact the quality manager, who will review the suggested change(s), seek the relevant approval(s), update and re-issue.

Table of Contents

INFORMATION SECURITY MANAGEMENT SYSTEM POLICY
SCP-P-070

1. AIM

The objective of information security is to ensure the business continuity of SecureCloud+ and to minimize the risk of damage by preventing security incidents and reducing their potential impact.

2. POLICY STATEMENT

The Board and Management of SecureCloud+ are committed to preserving the confidentiality, integrity and availability of all the information assets throughout the organisation in order to maintain our competitive edge, cash flow, profitability, legal and contractual obligations and most importantly to protect our reputation. Information and information security requirements will continue to be aligned with organisational goal, and the ISMS is intended to be an enabling mechanism for information sharing for electronic operations, for e-commerce and reducing information related risks to acceptable levels. All employees of the organisation are required to comply with this policy. Certain third parties, as defined in the ISMS, will also be required to comply with it. This policy will be reviewed if significant changes in the ISMS occur or at least annually at the management review.

3. GOALS

- Returning value to Shareholders and other Stakeholders by increasing the value of the Company, and making wise investments, this will be achieved by
  - Creating a successful brand and developing our own intellectual property.
  - Win and retaining enduring services contracts.
  - Extend our footprint into other markets.
- Meet our revenue and profit target for Financial growth by
  - Exploit existing services and develop incremental high margin services.
  - Careful resource planning to meet demand.
  - Using targeted marketing to create awareness and lower our overall cost of selling.
- Embedding quality, security and Environmental planning in everything we do by
  - Provide consistent quality in the delivery of our services, design, development, engineering, onboarding and training.
  - Extend the breadth and depth of our policies, processes and procedures documentation.
  - Monitoring and continually improving our quality documentation.
  - Demonstrate our competency externally by obtaining relevant certifications and accreditations.
- Attract, retain and grow
  - Become Employer of choice – Talent attraction and Retention
  - Invest in our people and grow our own.
  - Proactive approach to resource planning.
  - Create value through reward and recognition.

Objectives will be derived from the above set goals.

All actual or suspected information security breaches will be reported to the Security Controller and will be thoroughly investigated.

4. GOVERNANCE

The CEO will chair a management group to support the ISMS framework and periodically review the ISMS systems at the management review, the management structure will be:

Chairman	CEO	Overall responsibility
Management Representative	Quality Assurance Manager	Lead implementer, responsible for ensuring the ISMS conforms to ISO 27001 and reporting on the performance of the ISMS to senior management.
Senior Management	Chief Operating Officer	Responsible for overall operations of the business
Security	Head of Security & Security Network Ops.	Responsible for the company conforming to internal and external security requirements
Occasional:		
HR	HR Manager	Responsible for HR and HR policies & procedures
Custodians:		
Asset Owners	Various	Responsible for the defined company asset
Risk Owners	Various	Responsible to ensure asset risks are mitigated

5. ASSETS

Assets relating to information security will have been identified and owners should be of appropriate seniority to reflect the value of the asset, they will be responsible for:

- The whole information lifecycle of the asset.
- Ensuring that the asset is inventoried, and that this inventory is used during the risk assessment to ensure Confidentiality, Integrity and Availability.
- Maintaining, reviewing and implementing controls across the assets lifecycle.
- Establishing criteria for the acceptable use of the Asset.
- Ensuring appropriate Information Classification is applied.

The following Information Assets have been identified:

- Staff / People (Knowledge)
- IT & Process Hardware & Software (Computers, operating systems etc.)
- Information (Databases, system files, paper documentation etc.)
- Infrastructure (Power, Connectivity etc.)
- Services (E-mail, Dropbox, etc.)
- Intangibles (Reputation, Corporate Image etc.)

6. REVISION / APPROVAL

Signed Date: 28th June 2023 Revision: 11.0

Peter Williamson CEO