SIGNAL ALLIANCE TECHNOLOGY HOLDING

Information Security Policy
(SATH-ISMS0501)

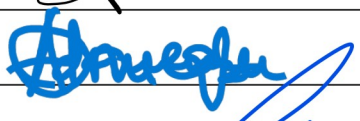
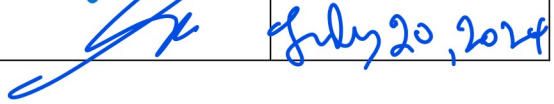
Document Identification

DOCUMENT REF	Information Security Policy
VERSION	1
DATED	7th July 2024
DOCUMENT AUTHOR	Bakare Faruq
DOCUMENT OWNER	Information Security Management

Reviews & Approvals

This Information Security Policy document has been reviewed and approved by the undersigned:

Approval

DESIGNATION	SIGNATURE	DATE
Group Head, Human Resources		July 16, 2024
Chief Information Officer		July 10, 2024
Group Executive Director		July 17, 2024
Chairman, SATH		July 20, 2024

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	15th July 2022	Bakare Faruq	Initial Version

Distribution

NAME	TITLE
Versions 1	All Staff

1 Contents

1 Introduction

Signal Alliance Technology Holding, SATH, is committed to adding value to its stakeholders through its service offerings including technology consulting, cloud technology, business applications, cybersecurity, and software development.

SATH top management is committed to ensure that its business operates smoothly and that its products and services satisfy requirements of the Integrated Management System (information security management system ISMS, business continuity management system BCMS and quality management system QMS) for the benefit of its customers, shareholders, and other stakeholders.

Whist it doesn't give any absolute guarantees of security, an ISMS can contribute significantly towards keeping our information safe and delivering many of the following benefits to SATH:

- Significantly reduced risk of reputational damage, legal penalties, or business revenue due to loss of sensitive or Personally Identifiable Information (PII)
- Peace of mind assurance to our customers, staff, board members, suppliers, and other interested parties that their data is secure.
- An ability to bid for and respond to tenders for business where ISO/IEC 27001 certification is a requirement.
- A public demonstration that SATH takes information security seriously.
- Internal and external recognition of the quality of the information security controls in place.
- Year-on-year improvement in the security of our (and our customers) information assets because of the continuous improvement aspects of the standard
- A strong move away from reactive firefighting towards proactive security incident reduction.
- Better alignment of information security controls with the needs of the business and our customers through regular review meetings with interested parties.
- Better perception and awareness of information security issues within the business, our customers, and the internal IT user population.
- An improved ability to manage information security breaches if they do occur, so reducing reputational damage and limiting business impact to us and our customers.

This Information Security policy document defines SATH's overall policy regarding Information Security that is appropriate for SATH's strategic business aspirations and delivery model, and includes:

- A framework for setting Information Security objectives
- A commitment to satisfying applicable requirements
- A commitment to continual improvement of the ISMS

This policy will be communicated within the organisation and to all relevant stakeholders and interested third parties.

2 Information Security policy

2.1 Setting Information Security objectives

The high-level objectives for Information Security within SATH are defined within the document *Integrated Management System Context and Requirements document*.

These overall objectives will used as guidance in the setting of lower level, more short-term objectives for Information Security planning within an annual cycle timed to coincide with organisational budget planning. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the overall business requirements and how they may change during the year.

Information Security objectives will be documented in *the Integrated Management System Plan* for the relevant financial year, together with details of a plan for how they will be achieved. Once approved, this plan will be reviewed on a quarterly basis as part of the management review process, at which time the objectives will also be reviewed to ensure that they remain valid. If amendments are required, these will be managed through the organisational change management process.

2.2 Commitment to satisfying applicable requirements

Commitment to the delivery of Information Security extends to SATH's top management which is demonstrated through this Information Security Policy and the provision of appropriate resources to establish and develop the Information Security Management System.

Top management will also ensure that a systematic review of performance of the programme is conducted on a regular basis to ensure that quality objectives are being met and quality issues are identified through the audit programme and management processes. Management Review can take several forms including departmental and other management meetings.

Within the field of Information Security Management, there are a few key roles that need to be undertaken to ensure the success of the ISMS and protect the business from risk.

The Information Security manager shall have overall authority and responsibility for the implementation and management of the Information Security Management System, specifically:

- The identification, documentation and fulfilment of applicable requirements
- Assigning authorities and responsibilities for the implementation, management, and improvement of ISMS processes
- Integration of business processes with the ISMS
- Compliance with statutory, regulatory and contractual requirements in the management of assets used to deliver products and services
- Reporting to top management on performance and improvement of the ISMS

It is also the responsibility of the Information Security manager to ensure that employees understand the roles they are required to fulfil and that they have appropriate skills and competence to do so.

SATH will ensure that all employees involved in Information Security management are competent based on appropriate education, training, skills, and experience.

The skills required to ensure Information Security will be determined and reviewed on a regular basis together with an assessment of existing skill levels within SATH. Training needs will be identified, and a plan maintained to ensure that the necessary competencies are in place.

Training, education and other relevant records will be kept by the HR Department to document individual skill levels attained.

SATH makes use of various third parties, both internal and external, in the delivery of products and services to its customers. Where this involves the operation of a business process, or a part of the process on behalf of SATH, that falls within the defined scope of the ISMS, this is identified in the *IMS Plan*.

In all cases, SATH will retain governance of the relevant ISMS processes by demonstrating:

- Accountability for the process
- Control of the definition of and interface to the process
- Performance and compliance monitoring
- Control over process improvements

This will be evidenced by documents and records such as contracts, meeting minutes and performance reports.

2.3 Continual improvement of the ISMS

SATH's policy with regard to Continual Improvement of the ISMS is to:

- Continually improve the effectiveness of the Information Security Management System across all areas within scope
- Enhance current processes to bring them into line with good practice as defined within ISO 27001:2022
- Achieve ISO 27001:2022 certification and maintain it on an on-going basis.
- Increase the level of proactivity (and the business perception of proactivity) regarding the on-going management of Information Security
- Achieve an enhanced understanding of, and relationship with, the business units to which the ISMS applies.
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data and feedback from relevant sources

- Obtain ideas for improvement via regular review meetings with stakeholders and document them
- Review ideas for continual improvement at regular management meetings in order to prioritise them and assess timescales and benefits

Ideas for improvements may be obtained from any source including customers, suppliers, employees, risk assessments and audits. Once identified they will be documented and evaluated by the staff member responsible for continual improvement.

2.4 Planning Changes to the ISMS

A need for change to the ISMS may arise from any number of sources, including the continual improvement process, events related to the internal and external context of the organization (such as internal re-organizations or mergers and acquisitions) or an increase or decrease in its scope.

Where changes arise, they must be carried out in a planned manner so that the required adjustments are approved and implemented in areas such as:

- Adjustment of the scope of the ISMS
- Allocation of resources
- Assignment of roles and their associated responsibilities and authorities
- Required competence levels
- Communication of the purpose and nature of changes
- Documented information required to support the change

2.5 Approach to managing risk

Risk management will take place at several levels within the Information Security Management System, including:

- Information Security management planning – risks to the achievement of objectives
- Information Security risk assessment
- Assessment of the risk of changes as part of the business change management process
- At the project level as part of the management of significant business change

High level risk assessments will be reviewed on an annual basis, or upon significant change to the business environment. For more detail on the approach to risk assessment please review the document *Risk Assessment and Treatment Process*.

Once in place, it is vital that regular reviews take place of how well Information Security management processes and procedures are being adhered to. This will happen at three levels:

1. Structured regular management review of conformity to policies and procedures within SATH
2. Internal audit reviews against the ISO 27001 standard by the Internal Audit Team
3. External audit against the standard to gain and maintain certification to ISO27001.

Details of how internal audits will be carried out can be found in the *Procedure for Internal Audits*.

2.6 Control of documents and records

All Information Security management policies and plans that form part of the ISMS must be documented. The way in which these documents are created and managed through their lifecycle is set out in *Procedure for the Control of Documented Information*.

All documents in the ISMS are uniquely numbered and the current versions are tracked – see document *Documentation Log*.

The keeping of records is a fundamental part of the Information Security Management System. Records are key information resources and represent evidence that processes are being carried out effectively.

The controls in place to manage records are also defined in the document *Procedure for the Control of Documented Information*.