SAHCO

INFORMATION SECURITY POLICY

Version 1.0

Document Control				
Document Title	SAHCO-ISMS-PR-Information Security Policy 1.0			
Document Number	3			
Date of Release	21\07\2025			
Revision Number	1.0			
Document Owner	Bukola Oyinloye			
Action	**Name**	**Position**	**Sign**	**Date**
Developed by	Adeyemi Obafemi	IT Support Manager	O.A	13\07\2025
Reviewed by	BUKOLA OYINLOYE	HEAD, IT	B.O	15\07\2025
	Oluchi Achinihu	MGR Compliance	O.A	16\07\2025
Approved by	Adenike Aboderin	MD\CEO	A.A	25\07\2025

Revision History				
Version Date	**Revision Date**	**Revision Author**	**Type of Amendment**	**Approval**
1.0				
2.0				
3.0				
4.0				

TABLE OF CONTENT

1. Introduction

This document establishes the information security policy of SAHCO Plc.

As a modern, forward-looking business, SAHCO Plc recognizes at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit if its customers, shareholders, and other stakeholders.

To achieve a continuous operation, SAHCO Plc has implemented an Information Security in accordance with the internationally recognized standard for information security ISO/IEC 27001:2022. These standards outline the requirements for an ISMS based on globally accepted best practices.

SAHCO Plc has made the decision to maintain full certification to ISO/IEC 27001:2022

This certification serves as independent validation by a Registered Certification Body (RCB), affirming the effective adoption of information security best practices. In addition, SAHCO has adopted the guidance provided in the codes of practice ISO/IEC 27017 and ISO/IEC 27018, as they hold relevance for Cloud Service Providers (CSPs).

2. Purpose

The Information Security Policy is written in pursuant to the ISO 27001:2022 Standard.

The purpose of the information security policy is to provide a framework for establishing suitable levels of information security for all SAHCO Plc information assets and to mitigate the information security risks associated with the theft, loss, misuse, damage or abuse of these information assets.

The following supporting documents are relevant to this information security policy and provide additional information about how this policy is applied:

- Information Security Risk Assessment and Treatment Process
- Statement of Applicability
- Supplier Information Security Evaluation Process

- Acceptable Use Policy
- Cloud Service Policy
- Mobile Device Policy
- Teleworking Policy
- Bring Your Own Device (BYOD) Policy
- Access Control Policy
- User Access Management Process
- Cryptographic Policy
- Physical Security Policy
- Anti-Malware Policy
- Backup Policy
- Software Policy
- Technical Vulnerability Management Policy
- Network Security Policy
- Email Policy
- Secure Development Policy
- Information Security Policy for Supplier Relationships
- Availability Management Policy
- IP and Copyright Compliance Policy
- Records Retention and Protection Policy
- Privacy and Personal Data Protection Policy
- Clear Desk and Clear Screen Policy
- Configuration Management Policy
- Secure Coding Policy
- Data Leakage prevention Policy
- Whistleblowing Policy

- Pseudomization and Anonymization Policy

Details of the latest version number of each of these documents is available from the ***ISMS Documentation Log***.

3. Scope

This policy applies to all systems, people and processes that constitute the corporation's information systems, including board members, directors, employees, suppliers and other third parties who have access to these systems.

It governs all information that is created, transmitted, processed, stored or disposed during the course of SAHCO Plc business, including the information assets and the systems used to create and maintain this information.

It applies to:

i. All SAHCO Plc staff, partners, suppliers and contractors with respect to the Corporation's information assets.

ii. Employees, representatives and stakeholders from other organizations who directly or indirectly support SAHCO Plc's information systems, including auditors and other external consultants;

iii. All physical and electronic information assets for which SAHCO Plc is responsible.

iv. The development, implementation, procurement, operation, support and any other activities involving the use of SAHCO Plc information assets.

4. Policy Statements

4.1 Information Security Requirements

SAHCO Plc relies on its information assets to support its operations and achieve its business objectives. The unauthorized use or risk occurrence involving these assets can lead to reputational damage, business

disruptions, and potential legal consequences for SAHCO Plc. Therefore, it is crucial that we prioritize the protection of the information we are entrusted with, adhering

to the principles of confidentiality, integrity, and availability, while meeting our business needs and complying with legal, regulatory, and contractual requirements.

It is therefore SAHCO Plc's policy to ensure that:

i. The confidentiality of corporate and customer information is assured.
ii. Sensitive information is protected against unauthorized access and the integrity of information is maintained.
iii. Information is made available to authorized business processes, employees, suppliers and other interested parties as and when required.
iv. The requirements of interested parties (including regulatory, contractual and legal requirements) are met.
v. Specific requirements with regard to the information security of new or changed systems or services is captured as part of the design stage of each project.
vi. The Company's ISMS controls implemented are driven by business needs and regularly communicated to all staff through team meetings and briefing documents.

It is the responsibility of **ALL staff members** to adhere to the requirements laid out in this policy, more specifically:

It is responsibility of **ALL staff members t**o:

i. Understand and comply with information security policies, procedures, and controls relevant to their roles.
ii. Protect the Confidentiality, Integrity and Availability of all SAHCO Plc information assets.
iii. Report any information security incident or breach for investigation in accordance with the existing incident management process.
iv. Participate in security awareness training programs and adhere to best practices.
v. Safeguard personal and sensitive data from unauthorized access or disclosure.
vi. Respect individuals' data rights and promptly address their requests.

vii. Collect and use only necessary personal data for valid business purposes.

viii. Obtain consent when required and process data only for specified purposes. ix. Secure approvals before sharing data with third parties.

x. Report any information security incidents for investigation in accordance with the existing incident response process.

xi. Participate in security awareness training programs and adhere to best practices.

It is responsibility of **ALL managers** to:

i. Implement this policy within their business areas, and make sure it is adhered to by their members of staff.

ii. Make sure that all staff within their business area undergoes appropriate security awareness and/or training in support of the goals of this policy.

iii. Ensure the building of an information security culture at SAHCO via effective application of information security controls and efficient process handling; and

iv. Ensure continual improvement of the ISMS through process refinement, risk mitigation controls enhancement, effective non-conformity handling and compliance to all associated regulatory requirements.

4.2 Framework for Setting Objectives

A regular cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified.

The following are the established information security objectives for SAHCO Plc:

- Ensure information security controls are fully implemented and are effective.

- Achieve 80% assurance in ensuring the continuity for SAHCO Plc's solutions regarding information security.

- Achieve 80% cybersecurity awareness within the Corporation by 2025
- Ensure the information security risks exposure is maintained within an acceptable level.
- Obtain ISO27001 certification by 2025 and maintain effectiveness of the ISMS.

These will be evaluated and monitored as part of management reviews to ensure that they remain valid. If amendments are required, these will be managed through the change management process. In accordance with ISO/IEC 27001:2022 the reference controls detailed in Annex A of the standard will be adopted where appropriate by SAHCO. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with information security and privacy risk treatment plans. For details of which Annex A, controls for ISO 27001 and Annex A, have been implemented, and which have been excluded please see the ***Statement of Applicability***.

In addition, enhanced and additional controls from the following codes of practice will be adopted and implemented where appropriate:

- **ISO/IEC 27002** –Code of practice for information security controls.
- **ISO/IEC 27017** – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

The adoption of these codes of practice will provide additional assurance to our customers and help further with our compliance.

4.3 Continual Improvement of the ISMS

SAHCO Plc is committed to upholding the highest standards of information security privacy, ensuring the lawful and responsible handling of personal and sensitive information in accordance with

applicable regulations and ethical principles. Therefore, SAHCO Plc has made the decision to maintain full certification to ISO/IEC 27001:2022.

- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis.
- Continually improve the effectiveness of the ISMS
- Enhance current processes in alignment with good practices as defined within ISO/IEC 27001, and related standards.
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to information security and data privacy.
- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions.
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data.
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties.
- Review ideas for improvement at regular management meetings in order to prioritize and assess timescales and benefits.

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.

4.4 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.

4.5 Information Security Policy Areas

SAHCO Plc defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and once formally approved, is communicated to an appropriate audience, both within and external to, the organization.

The table below shows the individual policies within the documentation set and summarizes each

policy's content and the target audience of interested parties.

Policy Title	Areas addressed	Target audience
Internet Acceptable Use Policy	Business use of the Internet, personal use of the Internet, Internet account management, security and monitoring and prohibited uses of the Internet service.	Users of the Internet service
Cloud Policy Computing	Due diligence, signup, setup, management, and removal of cloud computing services.	Employees involved in the procurement and management of cloud services

Mobile Device Policy	Care and security of mobile devices such as laptops, KIEMS Kits and smartphones, whether provided by the organization or the individual for business use	Users of SAHCO-provided and BYOD (Bring Your Own Device) mobile devices
Teleworking Policy	Information security considerations in establishing and running a teleworking site and arrangement e.g., physical security, insurance and equipment	Management and employees involved in setting up and maintaining a teleworking site
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities and system and application access control.	Employees involved in setting up and managing access control
Cryptographic Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management	Employees involved in setting up and managing the use of cryptographic technology and techniques
Physical Security Policy	Secure areas, paper and equipment security and equipment lifecycle management	All employees
Electronic Messaging Policy	Sending and receiving electronic messages, monitoring of electronic messaging facilities and use of email.	Users of electronic messaging facilities
Secure Development Policy	Business requirements specification, system design, development and testing and outsourced software development.	Employees responsible for designing, managing and writing code for bespoke software developments

Information Security for Supplier Relationships	Due diligence, supplier agreements, monitoring and review of services, changes, disputes, and end of contract.	Employees involved in setting up and managing supplier relationships
IP and Copyright Compliance Policy	Protection of intellectual property, the law, penalties and software license compliance.	All employees
Records Retention and Protection Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction and review.	Employees responsible for creation and management of records
Clear Desk and Clear Screen Policy	Security of information shown on screens, printed out and held on removable media	All employees

Table 1: Set of policy documents

5. Compliance and Enforcement

The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by the top management of SAHCO and must be complied with. Failure by an employee to comply with these policies may result in disciplinary action including termination or legal consequences.

6. Policy Review

This Information Security Policy shall be **annually** reviewed and updated to reflect changes in technology, legal requirements, business needs, and best practices.

The ISMS Manager shall ensure that all employees are informed of policy updates and changes.

Appendix: Distribution list

NAME	TITLE
VANESSA UANSOHIA	Head Corporate Communication