AFROSAI-E

Cyber Security Policy Guide

EXPOSURE DRAFT

DECEMBER 2023

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1.n	[name]	[dd/yy/mm]	[dd/yy/mm]	Initial Document

Issued in South Africa

First Edition (Exposure Draft), December 2023

Terms and Definitions

- Supreme Audit Institutions (**SAIs) Resources / Company's Resources**

  This policy includes SAI-provided voice communications services, voice mails, the company's Intranet and Internet connections, the local area network ("LAN"), the wide area network ("WAN"), wireless network, electronic mail and messaging, services accessed through or using personal mobile devices or data communications connections and all associated software and company documents.

- **Mobile Device**

  For this policy, mobile devices include smartphones, cell phones, and tablets.

- **Non-Smartphone (cell phone)**

  This policy includes any regular cell phone not considered a smartphone under the definition below.

- **Smartphone**

  For this policy, smartphones include IT-approved devices with an operating system allowing advanced capability, including but not limited to email, text, instant messaging, digital cameras, and media players.

- **Services**

  SAI deploys all mobile carrier services and mobile applications.

- **Mobile Applications**

  Software provided by SAI that is used to secure access to the company's data and company data that resides on a user's mobile device.

Glossary of Abbreviations

- AFROSAI-E – African Organisation of English-speaking SAIs
- COBIT – Control Objectives for Information and Related Technologies
- IT – Information Technology
- ISO – International Organisation for Standardisation
- IEC – the International Electrotechnical Commission
- BYOD – Bring Your Own Device
- ISMS – Information Security Management System
- OS – Operating system
- SAI – Supreme Audit Institutions

TABLE OF CONTENTS

1. Purpose

The Cybersecurity Policy Guide aims to support member institutions in developing cybersecurity policies tailored to their institutions. This document aims to guide member institutions on issues related to cybersecurity, drawing from the experiences of government and private-sector stakeholders. Further, it provides guidance and practices for member institutions to consider as they develop and implement security policies. SAIs that have already developed their policies can use this guide to review and enhance their cybersecurity policies.

2. Introduction

Effective organisation security requires a structured approach to security policy development, implementation, and management. Many organisations face difficulties developing, implementing, and maintaining policies addressing their business needs. Unstructured, unilateral, and unspecific policies have generally proved ineffective as mechanisms for managing information security activities and reducing organisational risk.

AFROSAI-E SAIs must take a structured approach to developing and maintaining security policies. In addition, they need to develop, implement, and communicate policies that meet organisation-specific risks and business needs that are appropriate for the organisational culture. Business and IT decision-makers must be involved in policy development and implementation.

2.1 Role of Cybersecurity Policies to Organisations

A cybersecurity policy is a precise and enforceable set of statements — articulated in one or more documents — designed to direct information security management and formalise the requirements for consistently implementing security measures. Security policies show management commitment to organisation information security, establish accountability, and define roles and responsibilities for policy compliance.

AFROSAI- E recommends that member institutions develop policies based on recognised standards, security best practices, and their own identified risks and business needs to define a standard of due care. These include ISO 27001, the National Institute of Standards and Technology (NIST), COBIT, etc.

These policies can raise overall and individual levels of security competency and ensure that employees and other stakeholders always perform their duties with due diligence and under all circumstances. Security policies also form the basis for organisation-wide information security awareness and training.

By establishing the organisation's standard of due care and effective security policies:

- Define appropriate behaviour by employees and other stakeholders (business partners, independent contractors, and external service providers).
- Communicate an organisation-wide consensus concerning security requirements and practices.
- Provide a foundation for human resources action in response to inappropriate behaviour and legal action (civil or criminal), where appropriate.
- Define requirements for security controls within the organisation.
- Provide management and other stakeholders, including auditors, with indicators for validating information security maturity and measures for regulatory compliance.
- Define the conditions under which information sharing and business application access are permitted.

2.2 Characteristics of a Good Policy

Cyber Security policies that are successfully implemented typically are:

- Concise and to the point.
- Developed to meet a business need or compliance requirement or address a realistic risk identified by the institution.
- Compatible with the institution's organisational culture and, therefore, likely to be widely accepted and supported.
- Well-communicated and accessible.
- Targeted at specific, appropriate audiences.
- Capable of being used to assess or measure security.
- Used as the reference for internal and external security audits (instead of generic auditor standards, such as the ISO/IEC 27002).

- Supported by management, as evidenced by formal sign-off, demonstrable compliance, overt support and communication, and support of the consequences for non-compliance.
- Not delayed unnecessarily during the approval process.
- Kept up-to-date and reviewed regularly for applicability and relevance.
- Changed only infrequently.
- Not developed in isolation from the requirements of the business.
- Not copied from the internet or other sources, then issued following a “rubber stamp” approval process.
- Specifically tailored to the institution’s unique needs, preferably based on an assessment of risk and considering business objectives, legal requirements, organisational structure and culture, employee awareness and the information technology that is deployed.
- Inclusive of inputs from general staff during the development process (comments, reviews, etc.) to promote ownership of policy.
- Security was tested regularly (penetrative tests, vulnerability assessments, and tabletop exercises to test incident response plans).

An effective security policy has:

- An explicit title and description.
- Clearly defined and communicated scope, applicability, and purpose (addressing risks, business needs, or compliance).
- A precise definition of roles and responsibilities for ensuring policy compliance.
- Defined ownership and custodianship (and related responsibilities).
- An evident and authorised mandate.
- A clear definition of non-compliance’s consequences may include disciplinary actions.

3. Creating a Security Policy Framework

The security policy process should include the following stages:

1. **Policy Development:** Defining the institution’s security policy requirements, as well as establishing the standards for policy documentation (for example, writing style, document structure and document naming conventions).
2. **Policy Approval:** The transition from identifying policy needs to an authorised management directive.

3. **Policy Implementation:** Soliciting and receiving executive support, business involvement, and developing an organisation-wide awareness, communication programme, and new employee training.
4. **Policy Compliance:** Assessing compliance with, and the effectiveness of, the established policy and taking action for non-compliance.
5. **Policy Maintenance:** Conducting formal policy reviews and establishing a change management process.

The process detailed here provides a formal, structured approach that will enable cybersecurity professionals across the member institutions to successfully develop, implement and maintain policies that contribute to reducing the overall risk within the institution.

3.1 Policy Development

A formal structure for developing and designing policies (and related guidelines, standards and procedures) will simplify policy document management, distribution and communication. A policy development structure comprises establishing a document hierarchy, establishing a policy catalogue, creating a formal process for writing the policy, defining a standard document structure, defining a standard document naming and document-numbering system, and establishing an appropriate writing system.

3.2 Policy Approval

A formal, clearly documented approval process that defines roles and responsibilities and process steps for the transition of policies from the original concept to an authorised management directive should be implemented. The same should be aligned to each SAI approval process.

3.3 Policy Compliance

Assess security policy compliance using formal, proactive processes by internal or external auditors or the information security team. Also, assess policy effectiveness to determine whether policies achieve their intended purpose. Defining key performance indicators (metrics) and compliance measurement criteria when writing and implementing policies.

When planning for policy and compliance assessments, consider certain key considerations. The SAI may perform independent regular evaluations, working closely with the business units and IT organisation in a non-threatening and collaborative manner to determine the reasons for non-compliance and to find ways to drive change and improve policy compliance or the policies themselves.

Auditors should assess an institution's internally developed policies against best-practice standards to ensure that internal policies meet a minimum standard and can be used as the audit reference.

3.4 Policy Review

Policies must be reviewed to ensure they are current and relevant to the information security programme. Different types of reviews have different objectives; each SAI is free to determine which type suites their needs:

- An annual review of the overall framework (the policy management processes and the catalogue of policies) is designed to ascertain whether the framework is meeting security and risk requirements efficiently and effectively.

- A scheduled review of individual policies (according to the review dates established for the policy) is designed to ensure that information in policies (for example, names, numbering, responsibilities and contact details) is accurate and that policy statements are complete and applicable.

- An unscheduled review before a scheduled review due date may be initiated because of a request from a stakeholder (for example, the internal audit organisation, a business unit or an external service provider) to address a specific need or as a result of new threats (perceived or assessed) or a changing IT or business environment.

- An internal or external audit review of policies in which auditors periodically review policies and policy management is designed to ensure compliance with specified requirements and generally accepted practices.

3.5 Change Management

After a review, policy changes may be required. If so, all policy changes should be managed formally and brought to the attention of the senior management (or relevant SAI function) for initial approval. From that point on, follow the prescribed approval process. The only exception is for a change that does not materially affect the control aspect of the policy (for example, changing grammar or spelling or adding or changing an author’s or owner’s name). Such changes do not need to go before the management board for re-ratification.

Maintain a change record in the policy document indicating the nature of the change and whether it requires management board approval. In some cases, policies that have not been updated may lose their relevance and need to be retired or superseded. This also requires formal approval, sign-off, and communication across the institution. When policies are superseded, indicate this in the superseding policy. Apply formal version control to all policy documents.

4. Creating Security Policy Documents

4.1 Introduction

A formal and structured approach to security policy document design, development and approval will help ensure institution-wide commitment to and compliance with policies. A critical component of security policy is creating and distributing effective policy documents.

4.2 Establish a Document Hierarchy

A document hierarchy enables the institution to present security policies that have been implemented or are in the planning stage and to link them according to a risk/security management theme. The hierarchy can be an effective communication tool for senior executives and business managers, service providers, end users, auditors, risk practitioners, and other stakeholders to explain which documents are in place and applicable to them.

A structured approach to developing policies will improve awareness and compliance because targeted audiences need to reference only the documents applicable to them and not lengthy, detailed documents. The following document types comprise the information security document hierarchy that a SAI may consider.

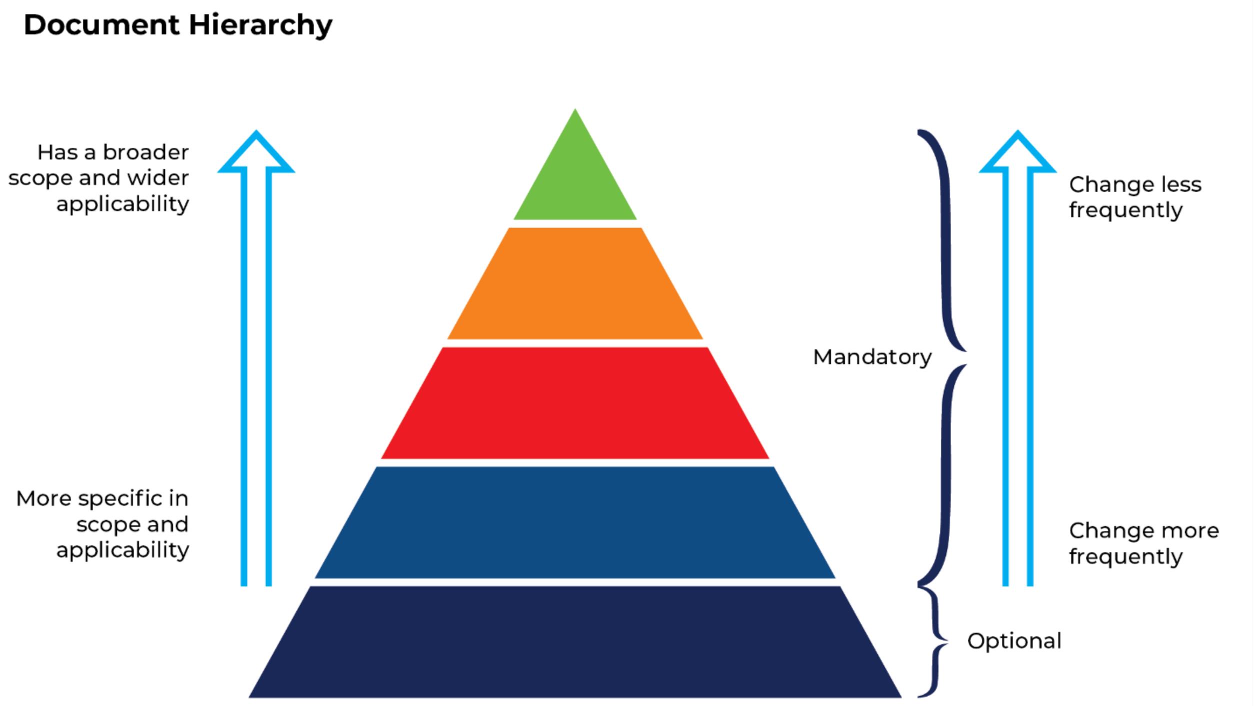
- **Cybersecurity charter**: The cybersecurity charter is a concise document positioned at the top of the document hierarchy, forming the capstone of security policy activity in the institution. The charter presents the institution's philosophy of information security and establishes a management mandate for and commitment to implementing that philosophy. This research identifies the business need for security, defines the scope of information security and lists the roles and responsibilities of the various security functions.

- **Security policies (generic or specific)**: Generic (or general) security policies apply to the complete scope of the charter — all the resources and individuals covered by the charter — and are the primary input for the information security programme. Specific security policies are rules that apply to specific domains (for example, applications, business units and regions) that must be complied with by all persons accessing these domains. A specific policy is usually linked with a generic policy.

- **Standards:** Cybersecurity standards specify mandatory, uniform uses of specific technologies, parameters, configurations and procedures. Examples include a standard operating system (OS) image for workstations, a standard configuration setting for intrusion prevention, a standard "hardening" procedure for networked servers and password standards that define the composition and characteristics of acceptable passwords.

- **Procedures:** Cybersecurity procedures provide detailed steps to achieve or complete a particular recurring task (for example, preparing user accounts and assigning appropriate privileges, running daily backups, and updating firewall rules).

- **Guidelines:** Cybersecurity guidelines provide additional (optional) advice in support of policies, standards and procedures, as well as general guidance on securing systems, what to do in particular circumstances and the responsible use of resources. Examples include guidance on sending large emails or sending emails to large distribution lists, discussing sensitive issues in public and the appropriate care for laptops and other mobile devices (see Figure 2).


Document Hierarchy
Has a broader scope and wider applicability
More specific in scope and applicability
Mandatory
Optional
Change less frequently
Change more frequently

**It must be noted that SAIs may have different ways of establishing the above document hierarchy within the SAI operating environment.*

4.3 Establishing a Policy Catalogue

Institutions may use a security policy catalogue to simplify the policy development process, especially when policies target specific audiences. A well-indexed catalogue of policy statements may be compiled from multiple sources - including materials available from the SANS Institute - and entered into a spreadsheet or database. (The catalogue may also contain standards, procedures, and guidelines.) A catalogue may be used in many areas of security policy, including:

- Policy development and change management: When a new security policy must be developed, or a current policy must be changed, required statements can be selected from the policy catalogue and inserted into the policy document. Each statement can be linked in the catalogue to the policy in which it appears or linked to specific audiences (for example, end users, administrators, and external service providers). This process can be automated so that an individual belonging to a specific group (or performing a specific function) is presented only with applicable policies and statements when accessing the policies via the intranet or SharePoint (or any other shared drive used by the institution.)

- Policy storage: A policy catalogue can store a comprehensive set of policy statements for future implementation. This repository will help institutions in the early stages of an information security programme to "phase in" policies. The catalogue will contain the full range of policy statements, only some of which will be published in physical documents. Individual policy statements may, optionally, be preapproved (but may not be included in a policy document until later in the security programme). If this is the case, the documents will not need to go through the approval process for later implementation.

- Policy consolidation and streamlining: Using a policy catalogue makes it easy to combine, reuse or otherwise consolidate security policies (for example, by combining an established internet policy, email use policy and end-user computing policy into a comprehensive acceptable use policy).

- Policy linking: A catalogue can be created from statements in the institution's information security charter or from a high-level generic policy to supporting statements in specific policies, standards and procedures.

- Policy metadata: A catalogue can be used to track information relating to policy development, such as sources of information or decisions in the approval process (see Figure 3).

Figure 3: Policy Catalogue

		Policy			
		Acceptable Use	**Electronic Comms.**	**Network Access**	**Remote Access**
1	A unique user access code shall be assigned to all company system users.		**x**	**x**	**x**
2	IT facilities shall be used only for authorised business purposes.	**x**	**x**	**x**	**x**

3	Only approved software shall be installed on equipment owned by the organisation.	**x**		**x**	**x**
4	The company's email system shall not be used for personal email.	**x**	**x**		
5	Laptop computers shall not be left unattended in public places.	**x**			**x**
6	System administrators must use two different forms of authentication when accessing the network.			**x**	**x**
7	Multifactorial authentication shall be used to access critical information systems.		**x**	**x**	**x**
8	Computer hard drives are to be encrypted to prevent access to data in case of loss or theft.		**x**		

**SAIs may have different processes of keeping track of policies/guidance, including security that may be used.*

4.4 Defining a Standard Document Structure

Most organisations develop their policy templates because no generally accepted standard exists. However, all policy documents should contain the following mandatory elements:

- Purpose of the policy in the context of overall Institution security, relevance, and risks addressed.
- Scope of the policy (what is covered, what is not, and to whom the policy applies).
- Roles and responsibilities of all stakeholders, identifying their specific responsibilities for any actions relating to the policy or information security in general, as well as their compliance responsibilities.
- Consequences of non-compliance (for mandatory documents in the hierarchy).
- Authorities who have approved the document.
- "Owner" or custodian of the document.
- Date of the next scheduled document review.
- What is the document's version number and the date of approval?
- Record any changes made to the document.

Other sections that should be considered in policies are:

- Glossary of terms and definitions that explain technical terms and acronyms.
- Document references (to other related policies, standards or procedures).
- Where is the authoritative source of the document stored?

4.5 Defining a Standard Document's Naming and Numbering System

No generally accepted standards for naming and identification exist. However, most organisations have established conventions for document management, including conventions for naming, numbering and version control. A formal standards document should be created to formalise these conventions for all business documents, not just those related to information security.

Certain principles should be considered when setting up cover pages, headers, footers, and other identifiers for policies, standards, procedures, and guidelines. The title should give a clear indication of the subject matter. The date and version information should indicate clearly when the document was approved or where it is in the approval cycle. Contact information for the owner or custodian should be included for questions and comments. If business units define or name their policies, then the numbering should consist of business unit identifiers.

4.6 Establishing an Appropriate Writing Style

When deciding on an appropriate writing style for policy documents, institutions must consider two key factors — organisational culture and target audience.

Organisational Culture

An institution's organisational culture and management style directly influence whether policies are accepted and complied with. In an institution with an authoritarian organisational culture, for example, policies are the norm for communicating management directives. These institutions' information security policies usually have a comparatively direct and commanding tone, with mandatory statements that use words such as "will", "must", and "shall" extensively. Policy development is typically noncollaborative in these institutions, with a strong emphasis on penalties for non-compliance. Policies tend to be approved quickly.

In institutions with a more participatory management style, policy language tends to be less authoritarian, with more extensive use of words such as “should.” A higher level of participation among business units during policy development is required to achieve consensus, which lengthens the development and approval process.

Institutions developing and implementing security policies can choose an appropriate writing style by considering the following questions about their organisational cultures:

- How much responsibility, authority and independence do individual employees have?
- Are employees empowered to make decisions, or must these decisions be referred to managers or more senior staff?
- Do managers provide clear communication, assistance, and support to their subordinates?
- Are employees encouraged to work in interdisciplinary teams that cross departmental boundaries?
- Do employees perceive the execution of their duties as being governed by rules, regulations, policies, procedures and working through channels?

Target Audience

Institutions must consider their target audience when deciding on the appropriate writing style for policy documents. For example, a policy targeted at end users will likely use different terminology from one geared toward IT operations personnel. The document should communicate the policy’s relevance and benefits to the targeted readers in the context of their working environments.

It is better to create separate, focused policies for different audiences than fewer and potentially longer policies with statements irrelevant to large audience segments. A key principle in the process is to keep the language as simple and unambiguous as possible so the reader knows what is intended.

5. Appendices

SAIs - List of Recommended Policies		
Sn	**Policy Name**	**Policy Description**
1	Cyber Security Policy	This policy aims to provide controls associated with protecting all information assets, including hardcopy documents, data, software, storage media, hardware, and communications networks.
2	Mobile Computing and Removable Media	This policy provides guidelines for remote access, device security and/or removable media.
3	Acceptable Use Policy	This policy provides minimum baseline security requirements for using SAI business IT assets, including networks, computers, data, etc.
4	Business Continuity Policy	This policy protects critical business processes from the effects of major failures of information systems or disasters and ensures their timely resumption.
5	Data Classification Policy	This policy aims to provide guidelines for data categorisation and the controls necessary to protect the data.
6	Legal/Regulatory Policy	This policy provides requirements for compliance with SAI-specific laws and regulations.
7	Cyber Security Incident Management Policy	This policy provides requirements for detecting, responding, and resolving cyber security breaches.
8	Access Control Policy	This policy provides guidelines for access controls/safeguards for SAI-specific premises, applications, databases, and networks.
9	Backup and Recovery Policy	This policy provides guidelines for backup and recovery procedures for key systems.

SAIs - List of Recommended Policies		
Sn	**Policy Name**	**Policy Description**
10	Vulnerability Management Policy	This policy provides guidelines for vulnerability management, i.e., tools to use, detective controls, remediation, etc.
11	Malware Protection	This policy provides guidelines for malware control tools, detection, and remediation.
12	Human Resources/Capital Policy	This policy provides guidelines for human resources management, including onboarding, during employment and separation controls.
13	Software Development and Acquisition Policy	This policy provides guidelines for software development and acquisitions life cycle.
14	IT Procurement Policy	This policy provides guidelines for procuring IT equipment, software, etc. The same should be aligned to the Software Development and Acquisition Policy.
15	Change Management Policy	This policy provides guidelines for managing changes: request, approval, testing, implementation, monitoring and evaluation.

Sample Information Security Policy – Template

Information Security Policy – Information Security Management System (ISMS)

Version	Approved by	Approval date	Effective date	Next review date
1.0	{Name of Approver]	[dd/yy/mm]	[dd/yy/mm]	[dd/yy/mm]

Policy Statement	
Purpose	To ensure that SAI information can be used when required with the confidence that it is accurate and complete and that it is adequately protected from misuse, unauthorised disclosure, damage, or loss. The policy reinforces the value of data and information to SAI. The IT Security Policy sets out management's information security direction and is the backbone of the SAI ISMS. The ISMS aims to proactively and actively identify, mitigate, monitor and manage information security vulnerabilities, threats and risks to protect SAI and its assets, information and data. The ISMS sets the intent and establishes the direction and principles for protecting SAIs IT assets. This enables continuous improvement of SAI security capability and resilience to emerging and evolving security threats.
Scope	This policy applies to all computer and network systems owned by and/or administered by SAI or operated by a third party for the benefit of SAI. This includes all locations where SAI's business is conducted, including data centres, corporate offices and customer contact centres. Similarly, this policy applies to all operations managed by SAI, and all computers, networks, devices used to connect to SAI, operating systems (regardless of size), data systems (e.g., Lightweight Directory Access Protocol [LDAP], Data Base Management Systems [DBMS], etc.), and all application systems whether developed in-house or purchased from third parties. This policy also covers all private and proprietary information assets and resources included in documents, conversations and all electronically stored, processed, transmitted, printed, and faxed information. Lastly, this policy applies to all regular and temporary, part-time or full-time employees, contract personnel, consultants, suppliers, vendors and other non-SAI employees.

Accountability	The successful implementation of SAI's information security policy cannot be achieved without company support; therefore, all SAI employees are accountable for compliance with this policy. Management is accountable for implementing and supporting this policy. All employees who in any way deploy, support, maintain, or contract services in technology are accountable for adhering to this policy and reporting suspected policy breaches/issues/problems to their management. All SAI private and proprietary information is provided to SAI employees, contractors, vendors and other authorised persons in strict confidence. Those with access to SAIs' confidential and proprietary information are accountable for safeguarding such information described in this policy and detailed in associated implementation standards, guidelines, and procedures.
Exceptions	It is recognised that with certain technologies, systems, platforms, products, etc., strict compliance with the SAI's information security policy may not be practical or reasonable to meet SAI's business needs. Exceptions may be made where the cost of compliance exceeds the overall risk or business benefit. If an exception is needed, the exception process must be followed to document the non-compliant item and plan for risk mitigation. Exceptions include a decision to eliminate, mitigate, tolerate, or escalate the risk. Once the inability to comply with the security policy has been established, a strategy must be documented to address the issue(s), including (at a minimum): An explanation of the risk(s); Rationale as to why the risk(s) should be tolerated or mitigated rather than eliminated; Alternate controls necessary to do so; and Endorsement/Approval by the management. SAI's management must approve any choice other than elimination.

Failure to Comply	In the absence of an approved exception, failure to comply may be considered a violation of SAI's policy and may result in appropriate disciplinary action leading to termination of employment or contract.

Policy Statements

Data Backup

Data Backups are primarily a preventive measure to protect against data loss from system failure (disaster or other), virus/malware attack, and system or human error. Backups are an essential control and safeguard to ensure the availability of SAI information being stored, processed or transmitted via information technology communication systems.

Statement: Data must be backed up regularly, protected from unauthorised access or modification during storage, and available to be recovered promptly during an incident or disaster. The custodians of the backup data itself should involve at least one (1) senior management staff to avoid collusion.

Data Security

SAI supports an extensively broad and complex data landscape. Based on appropriate data classification and handling guidelines, this policy and associated standard ensures that appropriate controls are implemented for the confidentiality and integrity of sensitive data.

Statement: Encryption techniques must be used for protecting sensitive data during transmission and storage.

Security Incident Management

Provides preventive, corrective and detective measures, ensuring a consistent and effective approach to managing information security incidents, including communication of events and weaknesses, such as breach of access.

Well-designed, understood tools and processes will help contain, preserve (legal/forensic purposes) and limit any damage from a security incident.

Statement: All IT systems must implement incident detection mechanisms like security event logging and antivirus. All potential security incidents must be handled appropriately following a formalised security incident handling process.

Vulnerability Management

All systems are susceptible to vulnerability (weakness) and are constantly threatened by malicious exploitation that may compromise the confidentiality, integrity, or availability of SAI information or systems, potentially resulting in productivity, reputational, or financial loss.

Vulnerability management involves alerting and responding to identified and potential violations or security threats in a timely, measured and prioritised (risk-based) manner to prevent or limit the damage. Vulnerability management is considered a preventive and corrective measure.

Statement: Security patch and vulnerability management processes must be in place to identify, prioritise and remediate security vulnerabilities on IT assets.

User Access Management

A preventive measure ensuring only authorised users are granted access to SAI systems. Unauthorised access could enable a malicious or accidental security breach.

Breach of access could lead to unwanted release or manipulation (Integrity) of sensitive information, potentially resulting in productivity, reputational or financial loss.

Statement: All user access-related requests (e.g., adding new users, updating access privileges, and revoking user access rights) must be logged, assessed, and approved by a defined user access management process.

Logging and Monitoring

Security devices such as firewalls, intrusion detection/prevention, security event incident management, mail content filters, and antivirus programs all generate log data.

The timely detection of information security incidents relies on comprehensive security log data from information technology communication systems.

Statement: Key security-related events such as user privilege changes must be recorded in logs, protected against unauthorised changes and analysed regularly to identify potential unauthorised activities and facilitate appropriate follow-up action.

Cloud Security

SAI is increasingly utilising cloud solutions to deliver business solutions and functionality to the business and our clients. This Policy and Standard explains what SAI expects of "cloud service providers" to meet security controls and access requirements to meet all SAI and its client's information and system controls.

This requirement is closely related to "Third Party Risk Management (See 5.20)". Cloud service providers have also been known to change practices with minimal notice. These impacts need to be managed or mitigated in our agreements to meet SAI service expectations.

Statement: SAI-endorsed cloud-based services must be consumed following a formalised risk assessment to identify the security controls that the Cloud Service Provider and SAI must establish to manage security risks to an acceptable level.

IT Asset Management

Asset/Inventory management is key to prudent security and management practices, providing context for all IT security policy statements and standard requirements.

Without an accurate inventory, processes such as vulnerability management are difficult to implement. For example, assessment of in-scope devices when responding to critical vulnerabilities may not be captured; hence, devices will remain unpatched and, therefore, exposed to malicious exploits.

Statement: In the context of this policy, an IT asset is the data, devices, systems, and facilities that enable the organisation to achieve business purposes.

Based on data classification, Asset Owners must implement appropriate ISMS and Data Handling controls to maintain the confidentiality, integrity and availability of SAI or its clients' data.

Change Management

The SAI IT, Change Management process ensures the stability and availability of related information technology communication systems across SAI. Secure practices, including reviews during changes, are necessary to ensure service availability.

Statement: Any change to SAI production information systems must be logged and assessed for security and risk impact as documented in the SAI Change Management Process. Each request's requirements, risk and result must be evaluated, and the proposed risk mitigation solution must be documented and approved.

IT System Acquisition & Development

IT systems (applications, databases, middleware) are susceptible to attack, so security controls must be embedded throughout the entire acquisition development lifecycle.

In conjunction with this and other controls, a multi-level approach to information security at each system layer must be taken, mitigating the security risk.

Statement: IT security requirements must be addressed within the software development lifecycle to reduce the risk of vulnerabilities being introduced during the acquisition or development of IT systems.

Web Application Security

Web applications are used extensively across SAI to deliver business services and information. They also represent one of the highest exposures to security attacks. Given the number of security exploits for web interfaces, secure design, implementation, and monitoring are essential.

Statement: Web applications must be designed, built and tested (verified) to ensure security is applied at all application and technology layers. Assessment and design guidelines provide controls to be followed when developing SAI internet-facing (Web) applications (Including Portals).

Physical Security

Physical security is important for critical infrastructure that must be protected from physical (theft) or environmental (fire, water) damage. Physical security is very much a preventive control.

Statement: The facilities (e.g., data centres, computer rooms, etc.) where critical information is stored or processed must be constructed and arranged so that data is adequately protected from physical and environmental threats.

Bring Your Own Device (BYOD)

Supporting "BYOD" provides choice and flexibility for SAI employees. This increases personal productivity and improved work experience, necessitating additional security controls and measures to protect the SAI information and systems.

This policy and associated Guideline recognises this need and provides the requirements to manage the risks associated with "BYOD".

Statement: SAI employees, interns and authorised users connecting personally owned devices to the SAI network must comply with secure practices to ensure the security of SAI networks and SAI data in their devices.

End-User Protection

SAI end-user devices are the primary gateway to SAI data and business applications. Implementing appropriate information security controls is necessary to mitigate the risk of inappropriate access to SAI data and IT systems, such as malware, information disclosure or loss.

Consequently, end-user protection ensures a robust, reliable, and secure IT environment. Failing to do so can result in an information security incident, causing financial and/or reputational loss to SAI.

Statement: End-user desktop computers, mobile computers (e.g., laptops, tablets), and portable computing devices (e.g., portable hard drives, USB memory sticks, etc.) must be protected with adequate security mechanisms to prevent the unauthorised disclosure and/or modification of SAI data.

Network Security

Network infrastructure and associated data links provide essential connectivity between internal and external systems. To provide mitigation against malicious activity, secure boundaries and connections need to be defined and managed in line with current security practices.

Statement: SAI network architecture must be commensurate with current and future business requirements and emerging security threats. Appropriate controls must be established to ensure the security of SAI data in private and public networks and protect IT services from unauthorised access.

IT Recovery

Service availability is critical for SAI's Information Technology communications, infrastructure, systems and applications. This policy ensures that processes are in place to ensure SAI's ability to recover from system and environmental failures, and regular testing of these processes is afforded.

Statement: An IT Recovery Plan and relative process must be in place to enable the recovery of business-critical SAI services promptly, to minimise the effect of IT disruptions and to maintain resilience before, during, and after a disruption. See IT Recovery Standard 816.

Information Security Risk and Compliance Management

Risk Management is at the core of the ISMS. Allowing SAI to identify, assess and evaluate risk, enabling effective management of information security vulnerabilities and threats to its information assets that could adversely affect or provide academic and business opportunities.

Statement: Information security risks must be identified, mitigated and monitored through a formalised risk management process.

Compliance with SAI ISMS must be measured and monitored to ensure that SAI teams and subsidiaries abide by ISMS's security controls.

Human Resources Security

Supporting human resources policies, this policy and standard defines the rules to be followed before, during and after all SAI employees' employment termination.

Statement: All SAI employees (Including interns), consultants, contractors, and third parties must be subject to appropriate security processes before, during and after the termination of their employment.

IT Acceptable Use

SAI embraces and relies on technology, the internet and digital media to conduct software development and business activities. This policy and associated standards outline the acceptable practices for SAI system users in using technology and accessing information sources and systems.

Statement: All users with access to SAI's IT systems and services must adhere to specific rules regarding using SAI resources, their internet and email usage, and social media interaction.

Third-Party Risk Management

Outsourced agreements should enforce appropriate information security controls concerning the nature of the contract, i.e., cloud services engagement, to ensure proper due diligence and risk management.

Statement: Security risks arising from SAI contracted third parties (i.e., suppliers, vendors, etc.) who maintain direct or indirect access to SAI IT systems and data must be operationally and contractually controlled.

Implementation

Implementing the IT security policy will be achieved by assessing existing IT Security Practices against the relevant ISMS controls and necessary remediation of any perceived deviations.

Roles and Responsibilities

Roles and responsibilities are set out in the SAI Security Roles and Responsibilities document.

Support and Advice

The contact for support and advice relevant to this policy is the *[insert appropriate email address].*

Review

The IT Security Policy is an active document and must be subject to independent review.
The Director of ICT will review this policy every three years from the effective date.

Acknowledgements

The following sources have been consulted for the development of this policy:

- ISO/IEC FDIS 27001:2022
- COBIT 5 for Information Security

Accountabilities	
Responsible Officer	Director ICT
Contact Officer	*[insert name]*
Supporting Information	
Supporting Documents	IT Security Standards
Related Documents	*[insert]*

Sign-off

By signing below, I acknowledge that I have read, understood, and agree to comply with the provisions outlined in this Cyber Security Policy.

Employee Name: _______________________

Date: ______________________

Signature: _______________________