Ministry of Communications & Information Technology

Information Security Policy

Definitions

Data	Data is referred to individual figures or numbers. It may consist of one entry or a collection of different values.
Information	Information is the result of analyzing and interpreting pieces of data. It describes data that is organized and presented in a meaningful form.
Digital assets	Anything that is stored digitally and is uniquely identifiable that is used to realize value. Examples of digital assets include documents, audio, videos, logos, slide presentations, spreadsheets and websites.
Information and Communication Technology (ICT) systems	An ICT system is a set-up consisting of hardware, software, data and the people who use them. It commonly includes communications technology such as the internet, telecommunications products (such as telephones), World Wide Web sites, office equipment (such as copiers and fax machines), etc.
Bring Your Own Device (BYOD)	Allows employees to use their personally owned devices for work-related activities. Examples include personal laptop, personal mobile phone, personal flash drive, etc.
Internet of Things (IoT)	Internet of things describes physical objects with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communication networks.
Third parties	A person or organization not involved directly with an organization's day to day operation, but has a minor role to play in the organization's operation.
ISO/IEC 27001	The international standard for information security. It sets out the specification for an effective ISMS (information security management system). ISO 27001's best-practice approach helps organizations manage their information security by addressing people, processes and technology.
Authentication	A process that ensures and confirms a user's identity.
Availability	Ensure that IT systems and data are available on a timely basis to meet business requirements.
Confidentiality	A set of rules that limits access or places restrictions on certain types of information.
Encryption	The act of converting information using an algorithm making it unreadable for unauthorized users.
Integrity	Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle.
IT assets	The IT assets in use by the Government of Samoa, including but not limited to: Server hardware, Desktop and laptop computers, Mobile / Smart phones and Tablet devices, Peripheral equipment (printers/scanners), Communications equipment (switches, routers, firewalls), Application software, Operating systems, Software for Infrastructure Services (Active Directory Authentication, Certificate Services, DHCP, DNS), Storage media (fixed and removable), Any other device connected to the MCIT network that is configured with an Internet Protocol (IP) address.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence (NIST 800-37).
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source (NIST 800-37).

Content

Introduction

Purpose

The purpose of this policy is to protect the information and data within the Government of Samoa (GoS). This policy ensures ongoing secure operation of the Government by protecting its data from unauthorized access, as well as to protect employees, customers and external parties.

This policy also provides a clear direction on standards and procedures in the event of a security breach or disaster. The processes outlined in this policy aims to guide Government organizations protect against threats to data, confidentiality, integrity and availability.

Given below are some of the challenges and issues this policy aims to address:

- Ransomware - The objective is to hold a company's data hostage until the affected user pays a specific dollar amount, which can often be hefty.
- Social Engineering - These tactics are designed to trick individuals into giving out sensitive or confidential information.
- Denial of Service (DDOS) - A distributed denial of service attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Scope and Applicability

This policy applies to:

- All agencies that operate under the GoS (Public Bodies, Government Ministries, Statutory Bodies, Constitution Authorities).
- Data and digital assets created and managed by all GoS agencies.
- All staff employed by the GoS, including contractors and external parties with access to GoS digital assets (e.g. videos, logos, audio etc), information systems, ICT network, data and information.
- Data and digital assets created and managed by all GoS agencies, including information, data and digital assets that may be managed by third parties or other outsourced arrangements.
- Any other devices that have not yet been captured (e.g. operational technologies, Bring Your Own Devices (BYOD), and/or Internet of Things (IoT)) yet that handle, transmit or process GoS data, or data pertaining to Samoan citizens or that otherwise provide government services.

Policy Exemptions

While the Information Security Policy (and its associated standards and procedures) applies to all systems and staff of the GoS, there may be instances in which compliance with specific security requirements is not applicable.

In the event an exemption from this policy is required, it is to be submitted in writing and recorded in the Government's risk register for regular review and reassessment. An agency shall request for an exemption and shall be granted or rejected by the CEO of MCIT, based on the advice of SamCERT.

Non-Compliance

All staff, contractors, third party service providers and users of GoS systems or IT assets are required to comply with the Information Security Policy and broader Information Security Framework.

Compliance with this policy shall be monitored internally, that is, by each respective GoS agency. Any employee who becomes aware of any violation or suspected violation of this policy must inform the Cybersecurity (SamCERT) division. SamCERT will be informed and where it is deemed necessary, may be escalated to the CEO of the MCIT to deal with.

Policy Overview

Protecting our information and data from a growing array of global cyber threats and malicious acts is integral to the GoS and its ability to perform its duties efficiently and effectively. The GoS and ministries IT environment consists of a large and complex array of applications and systems that allow us to effectively use, process and maintain the information entrusted to us. Any compromise to the confidentiality, integrity or availability of any of our systems or information could cause significant damage to the GoS's reputation on a global scale or significant harm to our employees or business partners.

This Policy supports the GoS commitment to protecting its people, information, intellectual property, assets, activities and facilities against the misuse, loss, damage, disruption, interference, or unauthorized disclosure. These objectives have been identified to ensure adequate security controls are applied to protect GoS IT systems, information assets and key Government processes. The information security Standards detailed within this Policy are designed to align with security best practices and align to the requirements of the ISO/IEC 27001 Information Management System and establish a strong security function and culture within the broader GoS agencies by providing them with directions for their information security practices and procedures.

The objectives of the Standards outlined within this policy to support the GoS (as well as any relevant procedures and guidelines), reflect the minimum requirements necessary to maintain an acceptable level of information security for protecting the GoS Information assets.

Policy Principles

The following key principles guide our approach to information security and further maintain the confidentiality, integrity and availability of information and information related assets:

Principle	Description
Establish foundations for information security across Government.	Establish consistent security documentation across GoS agencies to ensure that a foundation for information security is developed, and enables the whole of government approach.
Safeguards to data will be applied where necessary to protect from cyber threats.	Agencies will protect data that they hold through implementing safeguards to mitigate risks posed to them by cyber threats. Safeguards will include measures such as (but not limited to) patch and vulnerability management, authentication and access mechanisms, security awareness campaigns, and regular backups.

Security is a collaborative and shared effort.	Information security is about managing risk rather than 'policing' staff. To maintain the most secure environment, all staff should take reasonable steps to secure their own systems, exercise care in the communication and storage of sensitive information and have an obligation to respect the information and systems of other users. Security and related questions or practices, should be discussed openly and without judgement or fear of repercussion.
Access to information must be controlled.	Only those authorized to access relevant information should be able to do so. As such, access – remote, logical and physical – to assets (regardless of whether they be ICT systems, networks, infrastructure, devices and applications) must be controlled. However, this control should not impede information sharing with the Incident Response Teams, supporting GoS agencies and other relevant stakeholders.
Ongoing review of the GoS security approach.	The information security landscape is constantly evolving. Therefore, to maintain a secure posture, in addition to formal cycles for reviewing the approach to security, the GoS is constantly evaluating the effectiveness of security documents and processes and updating these, where required.
Establish and classify information.	All GoS agencies should ensure that information they hold is identified, classified commensurate to its value, and handled appropriately throughout the information's entire lifecycle. This will involve the labelling of assets with classifications/sensitivity labels (e.g. Official, Sensitive) and the implementation of minimum protections and handling requirements for data that is classified higher than "PUBLIC".
Only develop, procure or utilise robust, secure and approved ICT systems.	GoS agencies should ensure that all ICT systems used are secured and enable the secure storage, processing and transmission of government operations and data. This will involve ensuring ICT systems are managed and secured at all stages of their lifecycle, and approved when brought into the GoS environment.

Standards and Procedures

The Standards, procedures and guidelines outlined in this policy are intended on defining the intent behind and purpose of the documents that the broader information security framework and this policy are built upon.

These have been developed to provide staff with an understanding of the key elements that enable information security to be maintained across the GoS and direct them to sources where more information and specific requirements can be found. This facilitates a strong and consistent approach in protecting and securing information assets and associated IT environments across the GoS.

1. Information Security Risk Management

Understanding the risks within the GoS helps to understand the weaknesses in the environment and drive meaningful control deployment and expenditure to maximise risk mitigation.

A well-defined risk management framework provides a standard approach for the GoS to review strategic and operational activities and to facilitate a common understanding of risk management processes. This assists the GoS to document and analyze all possible risks for the organization and allows for a risk mitigation strategy to be defined to reduce risks to a level that meets or is lower than, the maximum tolerable risk level.

The objective of the risk management framework is to:

- Define the methodology for the assessment and treatment of risks in the GoS and define the acceptable level of risk.
- Apply risk management practices to enhance strategic, tactical and operational decision making.

Further information can be found in the *Risk Management Framework*.

2. Information Classification and Handling Standard

Information classification and handling is important to ensure the protection of various types of information from loss, unauthorized access or unauthorized manipulation.

This standard applies to all information assets that reside under the control of the GoS and supporting electronic and physical systems underpinning the information – whether maintained within the GoS systems, on premises, hosted or managed by contracted third parties.

Information will have an impact assessment conducted prior to being classified and is to be handled according to that classification. All GoS information must be protected with appropriate security controls based on its assigned classification.

Once assigned a classification, information classified as 'Confidential' must be reassessed every two years, and every year for 'Highly Confidential'.

A detailed classification scheme is defined in the *Information Classification and Handling Standard.*

3. Log Management and Monitoring Standard

Robust logging and monitoring is important to ensure potential attacks on the GoS IT environment can be detected and managed effectively and remedial action is able to be taken promptly to minimise potential damage that may arise.

The log management and monitoring process requires system time synchronization, continuous log review, minimum and system specific log requirements, event details to be logged by network and security infrastructure, and ensures the secure log storage, backup and retention of logs and the logging environment (with 3 months of logs available immediately for review).

A detailed explanation of the GoS logging and monitoring requirements and expectations are defined in the GoS *Log Management and Monitoring Standard*.

4. Malicious Code Standard

Malicious code refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of targeted information, applications, or operating system.

Requirements for establishing and maintaining controls, deploying anti-malware software and file integrity management (FIM), using host-based intrusion detection and prevention, content filtering and application whitelisting to prevent and detect the presence of malicious code within the GoS environment and minimise the likelihood of infection and propagation.

Requisites that will enable the GoS to secure systems from malicious software are further outlined in the *Malicious Code Standard.*

5. Network Infrastructure and Configuration Standard

Secure network infrastructure and configuration is integral for the GoS to maintaining a strong security posture for network assets and providing baseline security requirements for all systems and components.

A baseline level of device security for network equipment will be established, and the connection to GoS networks will be limited to authorised devices only. Networks and /or endpoints will be monitored continually to detect unauthorised connections and suspicious traffic. Where third parties have access to, or visibility of, GoS data and systems, they will be governed by the same security standards.

Requirements and procedures relating to network infrastructure and configuration are outlined in in the *Network Infrastructure and Configuration Standard*.

6. Patch and Vulnerability Management Standard

Patch and vulnerability management is recognized as one of the most critical methods to prevent malicious code impacting GoS software and systems.

Patching ensures that known problems and vulnerabilities that could be exploited by cyber attackers and which may impact the availability, integrity or confidentiality of our information assets are remediated promptly. Patch management is an ongoing process that requires the GoS to maintain inventory, identify and coordinate available and critical patches, evaluate and test the patch, deploy and address rollback and contingency measures.

Further detail regarding the roles, responsibilities and requirements associated with patch and vulnerability management are detailed in the *Patch and Vulnerability Management Standard*.

7. Incident Response Standard

Information security incidents impact the confidentiality, integrity or availability of information or systems. The Incident Management Standard defines the overall approach and processes for the GoS when managing an incident, enabling them to minimise any damage that could potentially occur.

Incident response and management is a phased approach involving discovery, validation and logging; identification; containment; eradication; recovery and root cause analysis; and follow-up. During all phases of the incident response process, considerations must be given to communications, ongoing improvement, monitoring and evidentiary requirements.

Further detail regarding the incident response process can be found in the *Incident Response Standard*.

Security Organization Roles & Responsibilities

Roles and responsibilities as they pertain to Information Security are outlined below:

Role	Description
MCIT CEO	The Chief Executive Officer will: ● Establish and maintain the MCIT information security program, ensuring it aligns with the GoS's strategic objectives to the government's strategy; ● Provide overview and guidance on information security related matters; ● Establish and foster a culture where cyber security and risk management is understood, accepted and applied/encouraged; and ● Monitor and provide advice on the effectiveness of this Policy to the SamCERT division, relevant Minister and Digital Transformation Committee.
MCIT SamCERT	MCIT SamCERT will: ● Oversee the responsible parties to the information security policy and their implementation of its requirements; ● Act as information security role models and ambassadors, and embody the requirements of this policy - encouraging other agencies to continue to improve their cyber security cultures and practices; ● Facilitate capacity building amongst agencies with regards to information security measures; and ● Ensure agencies are informed of the current, as well as emerging cyber security landscape, and relevant threats and threat actors.

MCIT Policy Division	The MCIT Policy division will: ● Provide advice around policy updates, approval and senior leadership approval ● Assistance in implementation of the policy ● Monitor the review of policies, standards and procedures to ensure documentation supporting information security practices are kept up to date and reviewed in a timely manner; ● Revise and review the Information Security Policy annually or more frequently as appropriate.
Heads of Ministries / Government Agencies	The Heads of Ministries and Government agencies will: ● Allocate roles and responsibilities as detailed in this policy ● Identify relevant assets requiring protection and information security controls, and ensure these are applied; ● Determine their agency's risk tolerance and appropriately managing assets commensurate to this determined appetite against relevant threats to their agency; ● Ensure staff comply with Information Security Policies and Standards and put in place (and monitor the efficacy of) measures to meet legal and regulatory obligations, where applicable; ● Collaborate with the MCIT and other agencies in Information Security matters and requirements; ● Monitor and provide advice on the effectiveness of this Policy to the Cybersecurity division, relevant Minister and National Policy Coordination Committee (NPCC); ● Implement regular cyber security awareness training for all employees, contractors and outsourced ICT service providers; ● establish and foster a culture where cyber security and risk management is understood, accepted and applied/encouraged; ● Conduct regular risk assessments, or when the legal or regulatory environment changes or significant additional cyber risks are perceived to arise; ● Ensure and encourage appropriate security measures in projects and engagements at their ministry; and ● Assist the identification of potential improvements in the information security approach taken at GoS.

Government Agency ICT Staff	ICT staff/ teams at each agency will: ● Cooperate with other agencies, SamCERT and the MCIT to complete information security related work; ● Conduct information asset identification, risk assessment and remediation; ● Ensure cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle (SDLC), including agile projects; ● Communicate and implement requirements to maintain information security and security measures at their agency and the Government more broadly; ● Identify and implement appropriate security measures in projects and engagements at their ministry; and ● Assist with the timely reporting and response of information security incidents
Audit & Compliance Committee	The Audit & Compliance Committee will: ● Supervise the implementation of various information security and privacy protection policies, standards and procedures, ● Ensure the effectiveness of Information Security documentation and procedures at defined intervals.
System Owners (inclusive of Ministry's who own systems)	The responsibilities of System Owner include, but not limited to: • Ensuring systems are added to the Government asset register; • Classify their information assets in accordance with the *Information Classification and Handling Standard;* • Ensure only authorised personnel have access to systems and that access is commensurate to their job requirements through the implementation of appropriate access controls; and • Monitor security risks and the effectiveness of security controls for each system in accordance with information security Standards.
All staff	The MCIT employees, contractors and third parties are responsible for: • complying with this policy, and any applicable supporting policies, standards, and procedures; • participate in whole-of-government cyber security exercises as required, and • reporting any suspicious activities or suspected security incidents, and any potential identified weaknesses.

Document Control

Version Management	
Current Version	4.0
Effective Date	
Review Date	
Classification	
Approved By	