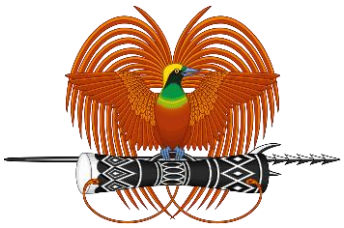

Papua New Guinea

Department of Information and Communications Technology

Government

Cybersecurity Standards, Guidelines and Best Practices

2023

Document Name	***PNG Government Cybersecurity Standards, Guidelines and Best Practices* 2023**
Prepared By	Department of Information and Communications Technology
Edition	Version 1
Approved by	Public Service ICT Steering Committee
Date Approved	26th May 2023
Effective Date	1st July 2023
Next Review Date	

Papua New Guinea Cybersecurity Standards and Guidelines **2023.**

ARRANGEMENT OF CLAUSES.

PART I. - PRELIMINARY.

1. Name.
2. Commencement.
3. Authority.
4. Introduction.
5. Simplified Outline.
6. Objectives of Standards and Guidelines.
7. Scope and application.
8. Existing frameworks.
9. Definitions.

PART II. - OFFICIAL INFRASTRUCTURE STANDARDS.

10. Overview.

Standard 1. - Critical infrastructure.

PART III. - SECURITY SOLUTIONS STANARDS.

11. Overview.

Standard 2. - Security Solutions.

PART IV. - INTERAL SECURITY POLICY STANARDS.

12. Overview.

Standard 3. - Internal Security Policy.

PART V. - MANDATORY RISK MANAGEMENT STANDARDS.

13. Overview.

Standard 4. - Risk management.

PART VI. - GOVERNANCE IN CYBERSECURITY STANARDS.

14. Overview.

Standard 5. - Governance.

PART VII. - CYBERSECURITY OPERATIONAL GUIDELINES.

15. Overview.

PART VIII. - INCIDENT RESPONSE GUIDELINES AND BEST PRACTICES.

16. Overview.

PART IX. - MISCELLANOUS.

17. Implementation Schedule.
18. Compliance and Monitoring.
19. Supplemental Standards and Guidelines.

APPENDICES.

PNG Government Cybersecurity Standards, Guidelines, and Best Practices **2023.**

PART I. - PRELIMINARY.

1. NAME.

This instrument is the Cybersecurity Standards and Guidelines 2023.

2. COMMENCEMENT.

This instrument commences on 1 July 2023.

3. AUTHORITY.

This instrument is made under Section 64 of the ***Digital Government Act*** **2022**.

4. INTRODUCTION.

(1) Cybersecurity standards and guidelines provide a framework of best practices and security recommendations for all public bodies to protect themselves from cyber threats, effectively manage and mitigate risks, and thus improving their cybersecurity posture.

(2) This instrument is based on existing international standards, guidelines, and best practices, and is consistent with the Digital Government Act 2022.

(3) This instrument was developed by the Department of Information and Communications Technology.

(4) The National Cybersecurity Policy 2021 establishes that the development of cybersecurity standards and guidelines may aid in defining common security requirements and the capabilities required for secure solutions.

(5) Through the Digital Transformation Policy, it is a must that we promote and foster a "safe, and secure digital space". This is supported by the National Security Policy 2013 which clearly strives to assist the government in making decisions and addresses the numerous security concerns the country is currently experiencing.

5. SIMPLIFIED OUTLINE.

(1) This instrument prescribes the cybersecurity standards and guidelines for public bodies.

(2) The cybersecurity standards set out in Parts 2 to 6 of this instrument are mandatory and all public bodies must adopt and apply these cybersecurity standards.

(3) This subclause sets out a brief description of these mandatory standards:

(*a*) Critical Infrastructure Standards: Part 2 describes the common basic infrastructure that all public bodies must incorporate into their cybersecurity infrastructure. The objective is aimed at establishing a common "set-up" across all government ministries, departments, and agencies; and

(*b*) Cybersecurity Security Solutions Standards: Part 3 describes standards for security solutions that must be adopted by all public bodies; and

(*c*) Internal Cybersecurity Policies: Part 4 describes standards for internal cybersecurity policies of public bodies; and
(*d*) Risk Management Standards: Part 5 describes the best practices for risk management in the government; and
(*e*) Governance Standards: Part 6 provides best practices for governance in cybersecurity.

(4) The guidelines set out in Parts 7 and 8, and best practices set out in Part 8 are recommendatory and all public bodies are recommended to adopt and apply the following to enhance their cybersecurity operations:

(*a*) Cybersecurity Operational Guidelines: Part 7 describes design guidelines that can be applied to all cybersecurity operations and are based on international best practices. These guidelines are aimed at enhancing cybersecurity operations; and
(*b*) Incident Response Guidelines and Best Practices: Part 8 provides a guideline and best practices for Incident Response Polices and strategies based on best practices as well as the existing NCSCs and CSOC.

(5) Public bodies must adopt and implement the National Cybersecurity Policy 2021 and the Papua New Guinea Digital Transformation Policy 2020.

(6) Notes included in this instrument are to help understanding by drawing attention to other provisions and provide information or explanations. The notes are in small type, so that they do not disrupt the text. They do not contain statements of law.

6. OBJECTIVES OF STANDARDS AND GUIDELINES.

The objects of these Standards and Guidelines are to -

(*a*) achieve a common security set-up across government; and
(*b*) facilitate a safe and secure digital space throughout the public sector; and
(*c*) increase the security of critical infrastructures, networks, data, and information technology systems; and
(d) continue building resilience in cybersecurity through the public sector.

7. SCOPE AND APPLICATION.

(1) This instrument establishes a cybersecurity framework for all public bodies.

(2) Cybersecurity standards and guidelines should not be limited to a single industry or sector.

(3) All public bodies must adopt this cybersecurity framework of mandatory standards and guidelines.

(4) Other bodies (non-government entities) may choose to adopt all or some of this cybersecurity framework of standards and guidelines.

8. EXISTING FRAMEWORK.

The following instruments will continue to apply to all public bodies:

(*a*) NIST Cybersecurity Framework; and
(*b*) ISO 27001 Information security management systems; and
(*c*) ISO 27002 Information security, cybersecurity, and privacy protection - Information security controls; and
(*d*) ISO 31000 Risk Management; and

(*e*) ISO/IEC 38505-1:2017 Information technology - Governance of IT - Governance of data - Part 1: Application of ISO/IEC 38500 to the governance of data.

9. DEFINITIONS.

In this instrument, unless the context otherwise requires -

"anti-malware" means a software designed to prevent, detect, and remove malicious software, such as viruses, spyware, and ransomware, from computer systems and networks;

"audit tools" means software tools that are used to analyse and monitor system logs, network traffic, and other data sources, to identify security issues, compliance violations, and other anomalies;

"audit logging" means a process of recording events, actions, and transactions in an information system to detect security breaches, policy violations, and other unauthorised activities;

"BIOS protection" means security measures that are implemented in the basic input/output system (BIOS) of a computer, to prevent unauthorised access and modification of the system firmware;

"Business Continuity Management" means the process of planning and implementing measures to ensure that essential business operations can continue in the event of a disruption, such as a natural disaster, cyber-attack, or other crisis;

"cloud security" means policies, procedures, and technologies used to protect data and applications hosted in cloud environments, such as public, private, or hybrid clouds;

"compliance" means the act of adhering to legal, regulatory, and industry standards and guidelines, such as data protection regulations, privacy laws, and security frameworks;

"Concurrent Session Control" means the ability to limit the number of active user sessions on a system, to prevent unauthorised access and reduce the risk of denial-of-service attacks.

"Critical Infrastructure Standards" means the standards and guidelines established to protect critical infrastructure, such as power grids, transportation systems, and financial networks, from cyber-attacks and other security threats;

"cybersecurity" means the practice of protecting computer systems, networks, and data from unauthorised access, theft, damage, and other security threats;

"Cybersecurity governance" means the policies and procedures that govern how organisations detect, prevent, and respond to cyber-attacks and ensures that a cybersecurity program is aligned with business goals, follows government or industry standards, and meets the leadership's security and risk management objectives;

"cybersecurity maturity" means the level of development and effectiveness of an organisation's cybersecurity program, based on its ability to prevent, detect, and respond to security threats;

"Cybersecurity operations" means the processes that help identify each public body's security capability;

"Cybersecurity Policy" means a formal document that outlines an organisation's security policies, procedures, and guidelines, and provides guidance on how to manage and protect its assets and data from security threats;

"Cybersecurity Standards "means the standards that define the security requirements and expectations of an organisation, to protect its assets and data from security threats;

"Data Diodes/Unidirectional Gateways" means hardware devices that enable one-way transfer of data between networks, to prevent data leakage and protect sensitive information;

"dial-up modems" means the devices used to connect a computer to the internet or a network, using a telephone line and a modem, which converts digital signals to analog signals and vice versa;

"DICT" means the Department of Information and Communications Technology
"digital government" means the use of technology, such as the internet, mobile devices, and digital platforms, to provide government services, information, and engagement to citizens and businesses;
"endpoint security" means the set of policies, procedures, and technologies used to protect the endpoints, such as desktops, laptops, and mobile devices, from cyber threats and attacks;
"firewall" means a network security device that monitors and controls incoming and outgoing network traffic, based on predefined security policies and rules;
"Governance in Cybersecurity Standards" means the set of policies, procedures, and practices that define how an organization manages and controls its cybersecurity risks, in accordance with industry standards and guidelines;
"IDS" means Intrusion Detection Systems;
"IPS" means Intrusion Preventive System;
"inbound/outbound connections" means the traffic that enters or leaves a network respectively. Inbound connections are typically monitored and controlled by firewalls and other security devices, to prevent unauthorized access and attacks;
"Incident Response Policy" means a documented plan that outlines the steps and procedures to be taken in the event of a security incident or breach, to minimize the impact and ensure the continuity of operations;
"Information Security Incident Management" means the process of identifying, analyzing, and responding to security incidents and breaches, to mitigate their impact and prevent future occurrences;
"Information System" means a set of components, including hardware, software, data, people, and procedures, that work together to process, store, and transmit information;
"Internet Service Providers" means companies that provide internet connectivity and related services to individuals and organisations, through various technologies, such as DSL, cable, fiber, and satellite;
"Intrusion Detection and Prevention" means the set of technologies and processes used to detect and prevent unauthorized access and attacks on computer systems and networks;
"malicious software" means software, code, or actions that are intended to harm or compromise computer systems, networks, or data, such as viruses, worms, and hacking attacks;
"Mobile Act" means a law or regulation that governs the use and protection of mobile devices, such as smartphones and tablets, in the workplace and other settings;
"NIO" means the National Intelligent Organization
"NCSC" means the National Cyber Security Centre, as established under Section 18 of the ***Digital Government Act* 2022** which is an institution jointly operated by multiple government departments and offices, including those responsible for defense, law enforcement, justice, intelligence, and Prime Minister and NEC matters;
"network architecture" means the design and layout of computer networks, including the physical and logical components, protocols, and services used to transmit and manage data;
"network security" means the set of policies, procedures, and technologies used to protect computer networks from unauthorised access, attacks, and other security threats;
"outsourcing contracts" means the agreements between organisations and third-party service providers, outlining the terms and conditions for the outsourcing of various functions, such as IT support, software development, and data management;
"patch management" means the process of managing software updates, or patches, to address security vulnerabilities and other issues in computer systems and applications;

"physical security" means the set of measures and procedures used to protect physical assets, such as buildings, equipment, and data centers, from unauthorized access, theft, or damage;

"Plant Certificate Authority" means the digital certificate that validates authority from the Manufacture;

"policies" means the formal statements of rules and procedures that guide the behavior and actions of individuals and organisations, such as employee conduct policies, IT security policies, and data protection policies;

"Procurement Process Standards" means the guidelines and requirements that organisations follow when procuring goods and services, to ensure that they meet quality, safety, and security standards;

"RTU" means Remote Terminal Units which are small devices used in industrial control systems and SCADA (supervisory control and data acquisition) systems, to monitor and control remote equipment and sensors;

"Risk Management Standards" means standards that organisations use to identify, assess, and manage risks, such as ISO 31000, NIST Cybersecurity Framework, and COSO Enterprise Risk Management;

"segregation of duties" means the practice of separating roles and responsibilities among different individuals or departments, to prevent conflicts of interest, fraud, and errors;

"segregation of networks" means the practice of separating computer networks and systems based on their function, sensitivity, or other criteria, to prevent unauthorised access and attacks;

"session time-out" means a security feature that automatically logs out a user after a period of inactivity, to prevent unauthorised access and protect sensitive data;

"system audit" means the process of reviewing and assessing a computer system's security controls, policies, and procedures, to identify vulnerabilities and potential security risks;

"system hardening" means the process of configuring a computer system or network to make it more secure and less vulnerable to cyber-attacks and other security threats;

"technical compliance" means the process of ensuring that a computer system or software application meets technical requirements and standards, such as those related to security, performance, and compatibility;

"Use Licensed Software Products Only" means a policy that requires the use of legally licensed software products, to avoid the risks associated with using pirated or unauthorised software, such as malware, security vulnerabilities, and legal liability;

"User Identification and Authentication" means the process of verifying the identity of a user who wants to access a computer system, application, or network, and granting access only to authorised users;

"Vendor Application Whitelist" means a list of approved software applications and vendors that an organization allows its users to download and install, to prevent the installation of unauthorised and potentially malicious software;

"WirelessHART Communication" means a wireless communication protocol used in industrial automation and control systems, to transmit data from sensors and control devices to a central monitoring system.

PART II. - CRITICAL INFRASTRUCTURE STANDARDS.

10. OVERVIEW.

(1) Critical infrastructure organisations that depend on Industrial Control Systems ("ICS") have begun using commercial-off-the-shelf ("COTS") technology developed for business systems in their everyday processes. This has provided an increased opportunity for cyber-attacks against the critical systems they operate.

(2) These COTS systems are not usually as robust at dealing with cyber-attacks as they are designed specifically for critical infrastructure dealing with cyber-attacks for many reasons. These weaknesses may lead to health, safety and environmental, or operational consequences that can severely affect Papua New Guineas' economy, people and the government.

(3) These standards establish a security baseline that specifies the minimal controls that must be implemented or addressed in any ICS system that has been determined as critical. This should be used in conjunction with a risk-based security management approach.

(4) These standards are mandatory.

Standard 1. - Critical Infrastructure.

STANDARD 1.1. - SECURITY POLICY STANDARD.

These standards give organizations that use ICS components direction for creating "defence-in-depth" strategies. Information on secure configuration, best practices, security policy, safe network architecture, and secure operating procedures is provided by these standards.

1.11 Security Policy	A public body's security policy document must be approved by senior management and published and communicated to all employees and relevant external parties, either as part of the organisation's information security policy or as a separate poicy.
1.12 Security Program Leadership	The senior management responsible for a public body's security must be identified by name, title, business phone, business address and date of designation. Changes to the senior management must be documented within 30 days after the date the change took effect.
1.13 Review of the Security Policy	To ensure its continued acceptability, adequacy and effectiveness, the security policy must be evaluated annually or whenever substantial changes occur.

STANDARD 1.2. - PROCUMENT PROCESS STANDARD.

(1) This procedure is used to monitor and improve the cybersecurity of devices, software, and services as they are acquired and integrated into utility operations, as well as supply chain risk management activities.

(2) These standards are intended to ensure that security principles are taken into account when purchasing control system products, as the overall security of any utility is heavily reliant on individual devices, applications, or services within that utility.

1.21 Procurement Language and Process`	The Procurement Language and Request for Proposal (RFP) must follow the guidelines in Appendix A.
1.22 System Acceptance	Acceptance criteria for new systems, upgrades and new versions must be established in accordance with an approved policy document and suitable tests of the system(s) carried out during development and prior to acceptance. All acquired systems must comply with the baseline controls in this document.
1.23 Outsourcing Contracts	The security requirements of a public body that outsources the administration or control of all or some of its systems, networks and desktop environment must be addressed in a contract agreed upon by both parties. The organisation must ensure that the third-party service delivery agreement or contract includes the baseline controls outlined in this instrument. This also applies to the third-party's subcontractors.

STANDARD 1.3. - ORGANISATIONAL SECURITY STANDARD.

The following set of standards provides recommendations that a public body must impose on its operations in order to safeguard sensitive data.

`1.31 Incorporating Public Body's Security	Management must incorporate the management of a public body's security within the organsational governance/security scheme or security program and explicitly acknowledge the public body's security responsibilities.
1.32 Public Body's Change Management	The public body must establish a dedicated change management committee that reviews and approves proposed changes. This committee must have representation from corporate IT as necessary.
1.33 Public Body's Security Coordination	A public body's security activities must be coordinated by representatives from different parts of the organisation with relevant roles and job functions, e.g., physical security, emergency response, corporate IT, etc.
1.34 Allocation of Responsibilities	All of a public body's responsibilities must be clearly defined.
1.35 Authorisation process	A management authorization process for a public body's new information processing facilities must be defined and implemented.
1.36 Confidentiality Agreements Requirements	Confidentiality or non-disclosure agreements reflecting the public body's needs for the protection of its information must be identified and regularly review, either as part of a contract renewal process or when considered appropriate.
1.37 Establishing Contact with Authorities	Appropriate contacts with relevant authorities must be maintained, including the CERT, NCSC, and emergency services.
1.38 Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums (e.g., NIO) and professional associations must be maintained.

STANDARD 1.4. - PHYSICAL AND ENVIRONMENTAL SECURITY STANDARD.

These standards ensure that the assets and resources of a public body are protected from tampering, damage, theft, or illegal physical access through physical and environmental controls.

1.41 Physical Security Parameter	Dedicated security perimeters (e.g., barriers such as walls, fences, card or biometrics-controlled entry gates or CCTVs) must be used to protect unattended areas that contain a public body's processing facilities.
1.42 Communication Medium	Extra/separate physical protections must be in place to protect the public body's distribution or communication lines from accidental damage tampering, eavesdropping or in transit modification of unencrypted communications. Protective measures include locked wiring closets and manholes, protected cabling duct and trays.
1.43 Display Medium	Controls for the physical access to devices that display a public body's information must be in place.
1.44 Device Usage	The public body must establish controls against the usage of personally owned mobile and portable devices within the control rooms and restrict them (as a default) unless they are explicitly authorised or they are owned, provisioned and audited by the public body.

STANDARD 1.5 - COMMUNICATION AND OPERATIONS MANAGEMENT STANDARD.

These standards ensure that information processing facilities are operating properly and securely.

1.51 Operational Procedures and Responsibilities	**(i) Documented Operating Procedures:** A public body's operating procedures must be documented, maintained and made available to all authorised users who need them. Vendors must supply the public body with the full documentation for any operating procedure required on their systems.
	(ii) Change in Management: Changes to a public body's information processing facilities and systems must be controlled and pre-approved by the internal change management committee. See item 1.32.
	(iii) Operational Facilities: Development, test and operational facilities must be physically separated to reduce risks of unauthorized or inadvertent access or changes to operational systems.
1.52 Third-Party Service Delivery Management	**(i) Service Delivery:** Public bodies must ensures that the security controls, service definitions and delivery levels included in third party service delivery agreements are implemented, operated and maintained by the third party in accordance with the terms and conditions set forth in the agreement.
	(ii) Monitoring and Review: The services, reports and records provided by the service provider must be quarterly nominated and reviewed and audits must be carried out quarterly.

	(iii) Management of Changes: Changes to the provision of services, including maintaining and improving a public body's existing security policies, procedures and controls must be managed, taking account of the criticality of systems and processes involved and re-assessment of consequent risk.
1.53 Patching and Protection Against Malicious and Mobile Code	**(i) Control Against Malicious Code:** Detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures must be implemented and documented. These controls include installing anti-malware software and whenever technically possible, using white-list of preapproved process.
	(ii) Anti-malware deployments: The public body's Anti-malware solution must be regularly updated with the vendor's latest published and approved malware (refer to the approved list) definitions or signatures. Whenever possible the public body environment should utilize a different Anti-malware product than the one used on the organisation LAN.
	(iii) Control against mobile code: Where the use of mobile code is authorised, the configuration must ensure that the authorised mobile cod operates according to a clearly defined security policy and unauthorized mobile code must be prevented from executing.
	(iv) Patch Management: The responsible entity, either separately or as a component of the documented configuration management process, must establish and document a security patch management program for tracking, evaluating, testing and installing applicable software patches for all the system assets (Including network components) in a timely manner as per the following: (*a*) The responsible entity must document the assessment of security patches and upgrades "for application" within 15 days after availability of the patch or upgrade from the vendor; ans=d (*b*) The responsibility entity must document the implementation of vendor approved security patches. If the approved entity must document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk. Internal procedures for applying critical/urgent patches or compensation controls must be developed in case the vendor cannot deploy critical patches in a timely manner.
	(v) Technical Vulnerabilities: Timely information on technical vulnerabilities (Including Zero-day Vulnerabilities) of information systems being used must be obtained, the public body's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

1.54 Backup	**(i) Information Backup:** Back up copies of information and software must be taken and restoration tested regularly (at least annually) in accordance with an agreed backup policy.
	(ii) Offsite Backup: At a minimum annual backup must be undertaken or as changes occur and these backups must be stored offside at a secure facility with full documentation for the offsite backup handling process. Backups must be encrypted if they are to be stored at a third party outside the jurisdiction of the ***Digital Government Act***.
	(iii) Equipment: The public body responsible must ensure the availability of critical equipment, backup components and spare parts.
1.55 Network Security and Management	**(i) Network Management:** Networks must be adequately managed and controlled, in order to be protected from threats and to maintain security for the systems and applications using the public body's network, including information in transit.
	(ii) Security of network services: Security features, service level agreements and management requirements of all network services agreement, whether theses services are provided in-house or outsourced.
	(iii) Network Architecture: A public body must utilise a three-tier network architecture (as a minimum) which include each of the following components in a physically/logically separate tier: (*a*) Corporatate/Enterprise LAN; and (*b*) DICT Shared DMZ; and (*c*) Public body's network (*d*) The architecture avoids single point of failures by means of equipment high availability, redundancy and alternate passes. A stateful firewall must be deployed between each of the above layers.
	(iv) Direct Connection: Internet connections must not terminate directly into the public body's network. In case of a time limited, continuously monitored and approved exception, a firewall must be used to isolate the public body's network form the Internet.

	(v) Inbound and Outbound Connections: Firewalls must be used to segregate and monitor corporate networks from control networks. The firewall base rule must be "*deny all, allow explicitly*". Inbound connections to the public body's networks must be limited. In exceptional cases where inbound connections are absolutely necessary, management sign-off on this risk must be obtained. Outbound traffic through the public body's firewall must be limited only to essential communications. All outbound traffic from the public body to the corporate network must be at a source and destination restricted by service and port using static firewall rules.
	(vi) Intrusion Detection and Prevention: An IDS/IPS solution must be implemented at the DICT's DMZ level to detect possible instructions from the corporate network and the public body should also deploy IDS/IPS within its network if technically supported.
	(vii) Remote Support Methods: Management or support traffic must be via a separate, secured management network or over an encrypted network/tunnel (Such as VPN) or with two-factor authentication (for example Username, Password and Token) for connections form the corporate LAN or third-party networks. Additionally, traffic must be restricted by IP address to specify management/support stations. Logs generated from remote connections must be kept for a period of not less than 90 days "where technically possible", Refer item 1.58.
	(viii) Wireless Devices: Wireless devices should be avoided in a public body's critical systems. Where this is not possible, the organisation must use authentication and cryptography for enhanced security mechanisms (at least utilizing WPA encryption for 802.11 x networks) to prevent unauthorized wireless access into the public body's system. Organisations must adopt the ISA100a, IEC62591 standards for wireless connectivity whenever possible. The wireless technologies include, but are not limited to microwave, satellite, packet radio (UHF/VHF) and 802.11x.
	(ix) Network Traffic: The allowed types (protocols/ports/applications) of the traffic must be defined, approved and documented.
	(x) Monitoring of Network Traffic: A public body must "continuously" monitor and retain its network (Layer 3 and 4) logs as a minimum for a period of not less than 90 days. In addition, a public body must ensure that the logs are centrally stored and managed. Refer item 6.9.

	(xi) Industrial Protocols: A public body's related protocols such as (MODBUS/TCP, EtherNet/IP and DNP3) must only be allowed within its Networks and not allowed to cross into the corporate network without explicit management approval.
	(xii) WirelessHART Communication: The WirelessHART network must meet the following security controls: (*a*) Ensure no interference on the allocated band spectrum. (*b*) The person responsible for Cybersecurity is connected directly through a dedicated connection to the network manager. (*c*) The network gateway firewall default configuration is "reject all". (*d*) Individual session keys for devices. (*e*) All devices pre-configured with the "join key". (*f*) Ensure the whitelisting - accessing control list (ACL) includes the individual keys and the globally unique HART address AES-128 encryption as a minimum. (*g*) The network gateway firewall default configuration is "reject all". (*h*) Individual session keys for devices. (*i*) All devices pre-configured with the "join key". (*j*) Ensure the whitelisting-access control list (ACL) includes the individual keys and the globally unique HART address AES-128 encryption as a minimum.
	(xiii) ZigBee Wireless Communication: The ZigBee network must meet the following security controls: (*a*) Network Infrastructure is protected with a network key. (*b*) Encryption security service is enabled. (*c*) Filtering done via MAC addresses. (*d*) Source node authentication enabled.
	(xiv) Data Historians and Related Services: A three-zone design must be adopted when implanting data historians where the public body utilizes a two-server model. One data historian server is placed on the public body's network to the corporate network mirroring the first server and supporting client queries.
	(xv) Dial-Up Modems: A public body must limit the use of dial-up modems connected to its networks. Where other alternatives are not possible, the following controls must be in place: (*a*) Default passwords must be changed. (*b*) Physically identify the modems in use to the control room operators. And make sure they are counted and registered in the approved Hardware inventory.

	(*c*) Disconnect the modems when not in use or set them up to automatically disconnect after being idle for a given period of time. (*d*) If modems are used for remote support, these requirements must be communicated to the support personnel.
	(xvi) Equipment Identification: Automatic equipment identification solutions (based on MAC address filtering as an example) at layers 3 and 4 must be used as a means to authenticate connections from specific locations and equipment. In addition, they must be used to detect rouge connections and devices.
	(xvii) Remote Diagnostic and Configuration: Physical and logical access to diagnostic and configuration ports (on ICS systems, field devices, sensors, antennas and communication devices) must be controlled.
	(xviii) Segregation of Networks: Information services, users, and information systems must be segregated on networks.
	(xix) Segregation of Duties: Segregation of duties for a public body's security operating personnel must be followed.
	(xx) Network Connection Control: For shared networks, especially those extending across the public body's physical boundaries, the capability of users to connect to its network must be denied. Named exceptions must be in line with the access control policy.
	(xxi) Data Diodes/ Unidirectional Gateways: A public body's systems must utilize the Data Diode / Unidirectional gateway technologies for additional security whenever only one-way communication is required and technically feasible.
	(xxii) Firewall Deployment: A public body must utilize a different firewall product than the one used on the corporate LAN, if supported by ICT vendor.
1.56 Media Hanling	**(i) Management of Removable Media:** Removable media (such as USB/CD/DVD) must not be allowed into the public body's control room or used within the system unless explicitly authorised by management. The removable media ports and drivers must be blocked by default. Where allowed, removable media must be scanned prior to use and/or restricted to a pool of sanitized media.
	(ii) Disposal of Media: Procedures for the handling and storage of a public body's information must be established to protect this information from unauthorised disclosure or misuse.

	(iii) Information Handling Procedures: Media must be disposed when no longer required, using the public body's formal procedures for safe and secure information sensitization.
	(iv) Security of System Documentation: A public body's system documentation must be protected against unathorised access or unauthorised disclosure.
1.57 Exchange of Information	**(i) Policies and Procedures:** Formal exchange policies, procedures, and security controls must be in place to protect the exchange of information using all types of communication facilities (Faxes, PSTN, GSM…etc.).
	(ii) Exchange Agreements: Agreement (Such as Non-Disclosure Agreements-NDA) must be established prior to exchanging a public body's information or data (in any form) between the public body and external parties.
	(iii) Physical Media in Transit: Media containing a public body's information must be protected against unauthorised access (e.g., by using encryption), misuse or corruption during transportation beyond the public body's physical boundaries. Details of acceptable encryption protocols and keys are specified in Appendix B.
	(iv) Electronic Messaging: Public body's information sent via electronic messaging must be appropriately protected by means of encryption as an example.
1.58 Monitoring	**(i) Audit Logging:** Audit logs, exceptions, and information security events where technically possible, must be produced and kept for 90 days to assist in access control and authorisation monitoring and to support any investigations.
	(ii) Central Logging: Logs must be kept and managed centrally on a dedicated logging infrastructure.
	(iii) Monitoring System Use: Procedures for regularly monitoring the use of public body's information processing facilities must be established and the results of the monitoring activities reviewed regularly, handled, or escalated as per the established procedures.
	(iv) Protection of Log Information: Logging facilities and log information must be protected against tampering and unauthorised access. A public body's logs must be stored both physically and logically separate from corporate IT logs.

	(v) Administrator and Operator Logs: A public body's administrators and operators' system access activities must be logged.
	(vi) Fault Logging: Faults must be logged, analysed, and appropriate action taken.
	(vii) Clock Synchronization: The clocks of all critical systems within a public body must be synchronized with an accurate (UTC or GMT+3) time source.

STANDARD 1.6 - ACCESS CONTROL STANDARD.

These standards define the controls that limit access to government information and assets.

1.61 Access Policy and User Access Management	**(i) Access Control Policy:** A public body's access control policy must be established, documented, and reviewed based on business and security requirements for granting access. The policy must be based on the *least privileged* and *personal/named accountability* concepts. Account management may include additional account types (e.g., role-based, device-based, attribute-based).
	(ii) User Registration: There must be for a public body a formal user registration and de-registration procedure in place for granting and revoking access to all related systems and services. This procedure must be communicated to the corporate IT and Personnel (HR) departments of the public body.
	(iii) Privilege Management: The allocation and use of privileges must be restricted and controlled. The responsible entity must ensure that individual and shared accounts are consistent with the concept of *need to know/need to share* with respect to work functions performed.
	(iv) User Password Management: The allocation of passwords must be controlled through a formal management process.
	(v) Password Complexity: For critical systems and as technically feasible, the public body must require and use passwords subject to the following: (*a*) Each password/pass phrase must be a minimum of 12 characters. (*b*) Each password must be changed at least annually, or more frequently based on the adopted risk assessment.
	(vi) Review of user access rights: Management must review user access rights at regular intervals using a formal process. Security personnel who administer access control functions must not administer the review/audit functions.

	(vii) Testing: The public body must implement a maintenance and testing program to ensure that all security functions under the "Access Control" section function properly.
1.62 Network and Operating System Access Control	**(i) Network Services Usage:** Users must only be provided with access to the public body's services that they have been specifically authorized to use.
	(ii) Secure Log-On Procedures: Access to a public body's systems must be controlled by a secure log-on procedure in line with its access control policy.
	(iii) User Identification and Authentication: All users or service accounts must have a unique identifier (user ID) for their sole and intended use only and a suitable authentication technique must be chosen to substantiate the claimed identity of the user/process. Except where it is technically impossible to utilize a person/named identification[2], the following must be maintained: (*a*) A recorded, valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria. (*b*) Compensating controls for automated user identification such as CCTV, Smart cards etc. (*c*) The public body specifically authorises and monitors the sue of gues/shared/anonymous accounts and removes, disables or otherwise secures unnecessary accounts. (*d*) The public body removes, changes disables or otherwise secures default accounts. (*e*) Account/shift managers are notified when users are terminated or transferred and associated accounts are removed, disabled or otherwise secured. (*f*) Account/shift managers are also notified when users usage or need-to-know/need-to-share changes. (*g*) In cases where accounts are role-based, i.e., the workstation, hardware and/or field devices define a user role, access to the ICS must include appropriate physical security controls, which can identify the operator and record time of entry/departure. [2] Identifier management is not applicable to shared public body accounts. Where users function as a single group (e.g., control room operators in legacy systems), user identification may be role-based, group-based, or device-based. For some systems, the capability for immediate operator interaction is critical. Local emergency actions for the ICS must not be hampered by identification requirements. Access to these systems may be controlled by appropriate physical security mechanisms or other compensating controls.

	(iv) Password Management Systems: Systems for managing or storing passwords of public bodies must be interactive and ensure and enforce strong passwords.
	(v) Use of System Utilities: The use of utility programs that might be capable of overriding system and application controls must be restricted and tightly controlled.
	(vi) Session Time-Out: Inactive sessions must shut down automatically after a defined period of inactivity.
	(vii) Concurrent Session Control: A public body's systems must limit the number of concurrent sessions for any given user or username in line with its policy on concurrent sessions.
	(viii) Limitation of Connection Time: Restrictions on connection times must be used to provide additional security for high risk, interactive user-to-system applications. The risk is to be defined as per the public body risk assessment process.
1.63 Field Device Access and Remote Terminal Units (RTU)	**(i) RTUs without Routable Protocols:** Devices such as Remote Terminal Units (RTUs) that do not use routable protocols are not required to be enclosed in the public body's physical security perimeter but must be enclosed and monitored within the electronic security perimeter.
	(ii) RTUs with Routable Protocols: Devices such as RTUs that use routable protocols must be enclosed within the public body 's physical security perimeter as well as the electronic security perimeter.
	(iii) Authenticating RTUs: Secured field devices must use cryptographic certificates issued or trusted by a plant certificate authority to ensure device identity.
	(iv) Direct Access to Field Devices: Any direct access to operational field devices that is made by field personnel must be provided in such a way that there are permission checks applied to that access. This includes personal accountability (e.g., record keeping with human identity) for any action via that access; and the resulting device state remains consistent with any copies of that state that are cached by the control system.
	(v) RTUs Access Logging: Secured field devices must provide the capability to detect and discard received messages whose reception timing, relative to the expected moment of their transmission, or whose sequence violates the quality-of-service characteristics of the communications session.

	(vi) RTU Communication Interface: Communication links to RTUs should be encrypted as specified in Appendix B Encryption implemented on the communication interface must not degrade the functional or performance capability of the operational function that has the authorization to access the RTU.

STANDARD 1.7. - INFORMATION SECURITY INCIDENT MANAGEMENT.

These standards ensure proper identification and management of security threats or incidents.

1.71 Incident Response Policy (refer to CIMA):	The responsible public body must develop and maintain its information security incident response plan to address at a minimum, the following: (*a*) Procedures to characterize and classify events as reportable security incidents; and (*b*) Procedures to properly and in a timely manner report security incidents to the appropriate management channels; and (*c*) Process for updating the incident response plan within 30 days for any changes in the reporting mechanism, organizational hierarchy, contacts, etc., and (*d*) Procedures to test the incidents response plan, at least annually. Tests can range from tabletop drills to full operational exercise scenarios to the response to an actual incident.
1.72 Reporting Security Weaknesses	All employees, contractors and third-party users of information systems and services must note and report any observed or suspected security weaknesses in systems or services. This can be achieved by formally including the requirements in their contracts, job descriptions, etc.
1.73 Contacting the Authorities	A public body must establish communication contacts as applicable with the national C-CERT (NCSC) for reporting incidents of criticality level one and the applicable critical infrastructure protection laws.
1.74 Incident Response Team	The responsible entity must designate an incident response team that has the appropriate skills and knowledge to manage and respond to security incidents. The incident response team should be composed of personnel from various departments, including IT, security, legal, and public affairs, among others.
1.75 Incident Reporting and Escalation Procedures	The responsible entity must establish incident reporting and escalation procedures that are consistent with the incident response plan. These procedures should ensure that incidents are reported promptly and accurately to the appropriate personnel and management channels, and that incidents are escalated to higher levels of management as necessary.

STANARD 1.8 - BUSINESS CONTIUITY MANAGEMENT.

These standards describe how to maintain business continuity after an incident or disaster has occurred.

1.81 Business Continuity and Disaster Recovery	The public body's Business Continuity Plan (BCP) must be a component within the corporate BCP and must include thefollowing items as a minimum: (*a*) Business impact classification and prioritization of the public body's assets; and (*b*) Required response to events that would activate the plan; and (*c*) Procedures for operating the systems' basic functionalities in a manual mode, until normal operational conditions are restored; and (*d*) Roles and responsibilities of the public body's BCP responders; and (*e*) Complete up to date documentation (manuals, configurations, procedures, vendors contact lists, network diagrams etc.); and (*f*) Personnel list for authorized physical and logical access to the systems; and (*g*) System components restoration order/sequence; and (*h*) Offsite backups recall and restoration procedures. and (*i*) Procedures for liaison with the appropriate authorities as per the public body's BCP.
1.82 Disaster Recovery Plan	A Disaster Recovery Plan (DRP) is a crucial component of a comprehensive Business Continuity Plan (BCP) that focuses on the recovery of IT infrastructure and systems following a disaster or significant disruption. To ensure that the DRP meets cyber security standards, it should include the following points:
	(i) Identification of critical IT systems and applications: The DRP should identify the critical IT systems and applications, including their recovery time objectives (RTO) and recovery point objectives (RPO). These objectives will determine the maximum acceptable downtime and data loss that can be tolerated during recovery.
	(ii) Strategies for backing up and recovering data: The DRP should include strategies for backing up and recovering data, including data replication, backup schedules, and recovery procedures. These strategies should be designed to ensure that critical data is not lost, corrupted, or compromised during the recovery process.
	(iii) Identification of key personnel and their roles and Responsibilities: The DRP should identify key personnel and their roles and responsibilities in the event of a disaster. This should include the establishment of a command center and the activation of the DRP. Key personnel should be trained to respond quickly and effectively to ensure the continuity of operations.

	(iv) Procedures for testing and updating the DRP: The DRP should include procedures for testing and updating the plan regularly. This should include regular testing of backup and recovery procedures and updating of contact lists and other documentation. This will ensure that the DRP remains up-to-date and effective.
	(v) Procedures for coordinating with external vendors and service providers: The DRP should include procedures for coordinating with external vendors and service providers, including cloud service providers and data centers, to ensure continuity of operations. This will ensure that critical IT systems and data are recovered quickly and effectively.
	(vi) Communication and notification procedures for stakeholders: The DRP should include communication and notification procedures for stakeholders, including customers, employees, and regulatory bodies. This will ensure that stakeholders are informed of any disruptions and can take appropriate actions.
	(vii) Procedures for securing the IT infrastructure and systems The DRP should include procedures for securing the IT infrastructure and systems during the recovery process. This should include monitoring for security breaches and implementing appropriate access controls. This will ensure that the recovered systems and data are secure and protected.

STANDARD 1.9. - COMPLIANCE.

The following standards describe compliance control that must be tested against a set of IT infrastructure to determine compliance. An organization is required to abide by any rules or specifications imposed by the organisation itself or by law.

1.91 Compliance	**(i) Identifying Application Legislation:** All relevant statutory, regulatory, and contractual requirements and the public body's approach to meet these requirements must be explicitly defined, documented, and kept up to date for each information system and the public body.
	(ii) Security Policies and Standards: Managers and senior staff must ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards including this document.
	(iii) Technical compliance: The systems of a public body must be regularly self-checked for compliance with security implementation standards, or guidelines including this document, at least annually.

	(iv) Monitor and Audit Data Retention: The auditee must keep the last audit report and all the related documents for at least two years from the date the report was received.
	(v) Levels of Non-Compliance: Audit findings require rectification in line with the following schedule: ➢ Level 1: minor non-conformities and observations must be rectified within 6 months. ➢ Level 2: major non-conformities must be rectified within 3 months and acknowledged by the senior management.
	(vi) Regular Training and Awareness: The public body must ensure that all employees, contractors, and third-party service providers who have access to its information systems receive regular training on relevant security policies, procedures, and best practices. This training should also include information on how to identify and report security incidents or breaches.
1.92 System Audit	**(i) Information System Audit Controls:** Audit requirements and activities involving checks on a public body's operational systems must be carefully planned and agreed to minimise the risk of disruptions to business operations.
	(ii) Protection of Audit Tools: Access to information systems audit tools of a public body must be protected to prevent any possible misuse or compromise.
	(iii) Audit Trail: To keep track of the actions of auditors and system administrators throughout the audit process, the independent audit should be kept intact. This trail may serve as evidence in investigations or disputes to show that no illegal changes or access were performed to the system.
	(iv) Separation of Duties: There should be a clear separation of duties between personnel responsible for conducting audits and those responsible for operating and maintaining. Information systems being audited. This ensures that audit results are objective and unbiased.

STANDARD 1.10. - SYSTEM HARDENING.

	(i) Vendor Application White-list: A public body must obtain and maintain a list of all applications, utilities, system services, scripts and all other software required to keep the public body's system operational (i.e., High risk assets).

	(ii) Software/Services to be Removed: All unnecessary software/services must be removed including but not limited to - (*a*) Games; or (*b*) Device drivers for hardware not included; or (*c*) Messaging services; or (*d*) Servers or clients for unused internet or remote access Services; or (*e*) Software compilers (except from non-production, development machines); or (*f*) Software compliers for unused languages; or (*g*) Unused protocols and services; or (*h*) Unused administrative utilities, diagnostics, network management and system management functions; or (*i*) Test and sample programs or scripts; or (*j*) Unused productivity suites and word processing utilities, for example: Microsoft word, excel, PowerPoint, adobe acrobat, open office, etc; or (*k*) Unlicensed tools and sharewares; or (*l*) Universal Plug and Play services.
	(iii) Restricting Bluetooth Access: Bluetooth wireless access technology must be denied by default.
	(iv) BIOS Protection: The BIOS (Basic Input/Output System) must be password protected from unauthorised changes.
	(v) Disabling Well Known/Guest Accounts: Default accounts and passwords must be disabled or changed to meet the complexity requirements of the public body. If it is not possible due to technical limitations, compensating controls must be implemented.
	(vi) Equipment Certification: Organisations must ensure that the ICS security devices utilised have achieved EAL (Evaluation assurance level) of 4+ as per the common criteria (ISO 15408).
	(VII) Privileged Access Management: The public body should implement strict controls for privileged access to its systems, such as limiting the number of privileged accounts and enforcing strong authentication mechanisms. This helps prevent unauthorised access and reduces the risk of insider threats. Additionally, all privileged access should be logged and regularly audited to detect any suspicious activity.
	(VIII) Regular Reviews: The public body should conduct regular reviews of its systems to ensure that any new software or services are added only after thorough assessment of their security risks and necessity. Similarly, any changes to existing systems should be reviewed and approved before implementation.

PART III. - SECURITY SOLUTIONS STANDARDS.

11. OVERVIEW.

(1) This Part is mandatory, and it describes the criteria for security solutions that must be adopted by all public bodies. These Part creates a basis of a strong foundation for securing government information and network protection.

(2) The security solutions that are adopted should improve security throughout the government. It is critical to emphasize that consistency across ministries, departments, and agencies, particularly in cybersecurity, is critical, and this can be achieved only by implementing highly recommended and certified security solutions.

(3) NCSC must have visibility of threats to be able to monitor for risks and incidents discovered by the Public Body's Cybersecurity Controls (Solutions). In addition, all critical incident alerts must be reported to NCSC. This standard must be followed by any public body that provides cybersecurity solutions to the public sector.

Standard 2. - Security Solutions.

STANDARD 2.1. - INTERNET SERVICE PROVIDERS.

(1) All public bodies must use an Internet Service Provider that has been approved and verified by the National Cybersecurity Centre.

(2) Figure 1 contains a list of all Internet Service Providers that have been approved and verified. All public bodies must select an ISP from this list.

Figure 1 NCSC-verified Internet Service Providers:

INTERNET SERVICE PROVIDERS		
	ISP Name	**Verified**
1	Telikom PNG Limited	Yes
2	Global Internet Limited	Yes
3	Datec (PNG) Limited	Yes
4	Emstret Holdings	Yes
5	Kinect Limited	Yes
6	Genesis Communication (PNG) Limited	Yes
7	PNG Dataco Limited	Yes

Note: Figure 1 does not show the order of preference. All of the listed ISPs were subjected to NCSC testing for specific criteria, which included national security, ownership, high availability, and maximum capacity to support NCSC operations. The services of each ISP are NCSC-verified, which means they meet NCSC standards and are of a high-quality. Each ISP is a well-known service provider in the country.

STANDARD 2.2. - ENDPOINT SECURITY.

(1) Endpoint security is frequently regarded as the frontline of cybersecurity, and it is one of the first places organizations look to secure their enterprise networks. Because they are the “bridge” between the central server and the “outside world”, endpoints are vulnerable to unauthorized access. As a result, it is critical that endpoints be protected.

(2) The demand for increasingly powerful endpoint security solutions has increased in tandem with the volume and sophistication of cybersecurity attacks. Endpoint protection systems nowadays are built to swiftly identify, analyse, stop, and contain active assaults. To do so, they must work together and with other security technologies to provide administrators with visibility into advanced threats, allowing them to respond faster to detection and remediation.

(3) Figure 2 shows recommended endpoint solutions that must be used by public bodies. It is from this list that each public body must choose one from, depending on which best fits organisational needs.

Figure 2 Endpoint Protections:

ENDPOINT PROTECTION				
	Endpoint Protection	**Description**	**Features/Details**	
1	Sophos	Sophos is one of the most common security solutions that are highly recommended by experts. It provides a security software called the Sophos Endpoint Security and Control which is basically a security software which provides clients with antivirus, firewall, network monitoring, web protection and intrusion detection systems as well as other required controls for web, data, and device. Sophos Endpoint Protection ensures against malware and other malware threats.	Operating Systems Compatibility	• Windows • MAC • Linux
			SIEM Capability	Provided by Sophos Central through a platform called Event Tracker. Event Tracker allows monitoring of both security (threat/unwanted application detection) and operation (web content filtering, addition/removal of endpoints and devices).
			Performance	Fast, simple, and easy to use.
2	Norton	Norton is a provider of antivirus solutions for various devices. It is important to note that Norton 360 is also a different security software to Semantics Endpoint Protection, although both belong to the same company.	Operating System Compatibility	• Windows 10, 11 • Mac • Linux
			Other features	Antivirus and malware protection, smart firewall, cloud backup, etc.
3	Kaspersky	Kaspersky's Endpoint Security is a highly recommended security solution, mostly compatible with Windows OS.	Operating System Compatibility	• Windows 10, 11
			Other features	Network Monitoring, Data Protection and backup, File Threat Protection, Mail Threat Protection, Network Threat Protection, and Web Threat Protection include technologies that shield users from viruses, phishing, and other types of threats.

(4) If any public body wishes to have other endpoint solutions, they are required to apply in writing to the Department of ICT Secretary stating their special solutions requirements.

(5) An additional solution is Microsoft Defender as it comes with the Windows operating system. It is one of the best ranked endpoint protections.

STANDARD 2.3. - FIREWALLS.

(1) Data theft issues have significantly risen over the years. It is through the use of a firewall that ensures data protection and fosters a safe and secure environment for confidentiality, integrity, and availability of data.

(2) It is important that there be a consistent variety of firewalls implemented across the government networks. The list in Figure 3 is a set of recommended firewall solutions for public bodies to select from.

Figure 3 Firewall solutions

FIREWALLS		
	Firewall	**Description** **-Features/Additional Details**
1	Sophos	Sophos is recognised for its user-friendly interface and strong performance. *Features include:* • NAT rules that are object-based. • Static, OSPF, BGP, and RIP advanced routing with full 802. • Support for 1Q VLAN. • Balanced SD-WAN links • Options for flexible bridging. • Support for IPv6 is certified.
2	Fortinet	Fortinet is a firewall solution that has garnered a strong reputation for its exceptional security features and high-performance capabilities. Features include: • Full visibility and threat protection • Real-time defense • Efficient Operational-wise • Complex yet cost-efficient

3	Cisco Meraki	The Cisco Meraki MX series firewalls are products with a good number of features that are simple to use and configure. Features include: • Identity-Based Firewall • Content Filtering • Automatic Updates • Intrusion Prevention • Industry Best Encryption Security • Automatic VPN • High Availability & Failover • Application Visibility & Control • Centralized Management Dashboard

STANARD 2.4 - INTRUSION DETECTION SYSTEMS.

(1) A public body or a business entity that hosts systems for public services must implement an intrusion detection system.

(2) Intrusion detection systems are crucial tools for network security since they help to detect and respond to malicious activity.

(3) This ensures there is an active system in place to notify personnel when an intrusion has occurred or is about to occur.

STANDARD 2.5 - WINDOWS 10/11 UPDGRADE.

(1) A public body must install Windows 10 or 11 Operating Systems and it must always be kept up to date.

(2) Microsoft's support for Windows 7 ended in January 2020 and without any support, devices using Windows 7 are more vulnerable to data theft, more specifically classified government data, if security patches are not applied on a regular basis. As a result, all network devices, particularly servers, desktops, and laptops, should have the most recent version of an operating system installed.

STANDARD 2.6. - KEEP SOFTWARE UP TO DATE.

All software used must be updated at least every two years or annually, or whenever a new version is released. Updates are released by software vendors to address security issues and improve functionality. Regularly installing updates addresses these flaws, enhances the protection against loss of money, data, and integrity.

PART IV. - INTERNAL SECURITY POLICY STANDARDS.

12. OVERVIEW.

(1) Security policies are crucial in all organizations because they provide protection for confidential data. Infrastructure, security solutions, and information security protocols must all be included in government cybersecurity measures. Developing and training employees on government security policy is also critical in protecting sensitive data.

(2) It is widely accepted that no matter how strong an organization's cybersecurity is, people are, in the end, the weakest link in any security protocol. As a result, the first line of defense in government information security is a solid government cybersecurity policy.

Standard 3 - Internal Security Policy.

STANDARD 3.1. - DEVELOP INTERNAL SECURITY POLICIES.

(1) All public bodies must develop internal security policies, and these must be circulated to all staff, and in turn, staff should be trained and familiar with each policy. These security policies must include regulations and procedures for cybersecurity, physical security, and cloud security.

(2) The following table lists all the security policies that should be created and their requirements. It is important to note that some of these policies have also been mentioned above in Standard 1 Critical Infrastructure, however, given their importance they are reiterated here again.

Figure 4 Internal security policies:

	Security Policy	Description
Cybersecurity		
1	Incident Response Policies	This policy must ensure that an organization has the controls in place to detect security vulnerabilities and incidents, as well as the processes and procedures in place to address them
2	Security Awareness and Training Policies	This policy must define measures for security awareness and training within public bodies. This ensures there is a program available that trains employees to be more cyber-aware, hence they are aware of the different types of ways they can protect themselves and the organization from cyber threats and cybercrime.
3	Access Control and User Management Policies	This policy must define measures for setting up, recording, reviewing, and changing access to systems and sensitive data. Refer to Standard 1.6 Access Control Standards and User Management.
4	Password Policies	This policy must define the rules and best practices for password creation and maintenance. These rules and practices include the following: (*a*) guidelines for creating, updating, and protecting access through strong and secure passwords; and (*b*) password complexity and length requirements; and (*c*) risks of not following length requirements and password complexities, as well as risks of reusing passwords; and (*d*) password log outs and maximum retry attempts and an outline of procedures for logging all unsuccessful login attempts.
5	Email Policies	This policy must define the rules and best and acceptable practices for email use.

6	Network Security Policies	This policy must describe how the security rules are applied throughout the network architecture, lays out the organisation's network security environment, establishes criteria for computer network access, and determines policy enforcement.
7	Backup Policies	This policy must establish measures designed to protect data and system backups, and also set rules for planning, executing and validating backups. This should also ensure that critical government data is backed up in a secure location. This must also include disaster recovery and file recovery procedures and plans. Refer to Standard 1.54 Backup.
Physical Security		
8	Physical Security Policies	This policy must establish measures that are designed to protect physical locations and the resources and equipment, information, and employees within those locations. This also includes procedures and strategy for standards listed in Standard 1.4 Physical and Environmental Security Standard, most specifically rules for granting, control, monitoring, and removal of physical access.
Cloud Security		
9	Cloud Security Policies	This policy establishes measures designed to protect the confidentiality, integrity, and availability of data stored, accessed, and manipulated through the use of cloud computing services.

(3) The public body must choose whether these policies are to be documented as separate policies or as a single document containing all these policies.

STANDARD 3.2. - ENSURE PROPER APPROVAL AND DOCUMENTATION OF ALL SECURITY POLICIES.

(1) All public bodies must make sure that each of the policies mentioned above in Figure 4 are properly documented and are available to employees and any other users.

(2) All these security policies must also be approved by senior management. If any changes are made, approval should also be sought from senior management for the changes. Refer to Standard 1.51 Operational Procedures and Responsibilities.

STANDARD 3.3. - REVIEW AND UPGRADE SECURITY POLICIES.

Public bodies must review and upgrade security policies accordingly, to be in line with the ever-changing cybersecurity scene.

PART V. - MANDATORY RISK MANAGEMENT STANDARDS.

13. OVERVIEW.

(1) This Part specifies a set of highly recommended strategic methods that should ensure proper risk management practices within the government.

(2) The main objective of this Part is risk reduction; therefore, these standards aim to identify risks and promote risk mitigation through international best practices.

(3) Risk management can assist public bodies in identifying, evaluating, reducing, or eliminating risk so that these risks have a lower potential impact on public bodies. Risk management affects every component of a public body, and it is completely reliant on the organizational security policy, which outlines the organisation's risk management strategy.

Standard 4. - Risk Management.

STANDARD 4.1. - RISK MANAGEMENT STRATEGY.

This strategy must provide a structured approach to addressing risks and must be adopted by all public bodies. Through a risk management strategy, the following can be achieved:

(*a*) Identify methods and procedures for evaluating and prioritizing cybersecurity risks and vulnerabilities.
(*b*) Define how each cybersecurity risk is prioritized as critical, depending on its severity and the impact it should have.
(*c*) Establish the risk tolerance of the public body.
(*d*) Define processes for dealing with monitoring and reviewing risk and vulnerabilities and how to improve this strategy.
(*e*) Ensure that all risks and vulnerabilities found are well documented and reported.
(*f*) Identify processes to reassess the organization's cybersecurity based on existing and documented risks and vulnerabilities.

By implementing such a strategy, the impact of cyberattacks can be reduced and the harm caused by cyber risks, lower operating expenses, protect assets and revenue, and improve the public body's image.

STANDARD 4.2. - CREATE A TEAM OF PROFESSIONALS.

There must be a team of cybersecurity professionals within each public body that are tasked with cybersecurity operations, or more specifically risk management. This is to ensure that risk mitigation is done by a group of highly skilled engineers and analysts.

STAMDARD 4.3. - DEVELOP AN INCIDENT RESPONSE PLAN.

An incident response plan must be present and defined in the risk management strategy. This gives the team instructions on how to handle serious security incidents, such as a data breach, ransomware attack, or sensitive information loss. The four phases of an incident response plan, as published by the National Institute of Standards and Technology (NIST) are -

(i) preparation; and
(ii) detection and analysis; and
(iii) containment and eradication; and
(iv) recovery, and post-incident activity.

All these phases are important in incident responses and should be covered in the plan.

STANDARD 4.4 - REVIEW AND UPGRADE INCIDENT RESPONSE PLAN.

The incident response plan must be reviewed bi-annually or annually and upgraded consistent with international best practices and to reflect the pace at which technology changes.

STANDARD 4.5 - TRAIN EMPLOYEES IN RISK MANAGEMENT AND CYBER AWARENESS.

(1) Employees of a public body that are not cyber aware pose a threat to the organization. All employees in the public sector should undergo risk management and cyber awareness training programs. This is to ensure that they know the risks, threats and how to keep safe online.

(2) Furthermore, information security policies should be made public, and all employees should be made aware of the cyberthreats. The goal is to raise employee awareness of ongoing cybersecurity threats.

PART VI. - GOVERNANCE IN CYBERSECURITY STANDARDS.

14. OVERVIEW.

(1) This Part prescribes the best practices for cybersecurity governance and help in maintaining cyber maturity.

(2) Public bodies can continue to improve their cybersecurity governance.

(3) There is a growing demand for security risk mitigation, compliance with security mandates, and effort management.

Standard 5 - Governance.

STANDARD 5.1. - ALWAYS ASSESS CYBERSECURITY MATURITY.

Even though a public body can have good cybersecurity practices, if those practices are not assessed then there is no way to know if they are effective or not. Therefore, public bodies should always assess their cyber maturity. This is important as it helps us to understand which areas are lacking, where improvements need to be made and the risks each public body is facing and where these need to be remediated.

STANDARD 5.2. - DEVELOP ACCOUNTABILITY FRAMEWORKS.

Accountability frameworks help in measuring and monitoring what a public body is doing and how well it is being done. Accountability is one of the main data protection principles and an accountability framework will help to deliver appropriate technical and organisational measures that should be taken in public bodies.

STANDARD 5.3. - ENSURE RISKS ARE PROPERLY MITGATED.

The four common risk mitigation processes are avoidance, acceptance, transference, and reduction/control. Risk mitigation creates a strong culture around risk management and prepares a public body for all potential risks and also ensures the development of plans to prevent those risks.

STANDARD 5.4. - COMPLIANCE.

A public body must ensure compliance in all cybersecurity aspects, including critical infrastructure and security solutions. In order to manage risks, the process of building and maintaining an IT governance framework ensures that cybersecurity initiatives meet corporate goals and objectives, conform to policies, standards, and internal controls, and assign authority, roles, and responsibilities.

STANDARD 5.5. - CREATE/REVIEW/UPDATE POLICIES, STANDARDS, FRAMEWORKS AND PROCEDURES AND PROCESS.

The policies, standards, frameworks, procedures, and processes of a public body relating to cybersecurity must be regularly updated or upgraded.

STANDARD 5.6. - INCREASE CYBERSECURITY TRAINING AND AWARENESS.

Public bodies must create more avenues for employees to be more cyber-aware and learn about the different cybersecurity policies, standards, and frameworks in place.

PART VII. - CYBERSECURITY OPERATIONAL GUIDELINES.

15. OVERIVEW.

(1) This Part prescribes guidelines to improve cybersecurity operations.

(2) The following guidelines are recommended.

GUIDLINE 1. - UNDERSTAND THE CURRENT CYBERSECURITY LANDSCAPE.

Technology is always changing and growing, and with it grows more risks. The threat landscape is constantly expanding, vulnerabilities are multiplying, technology is evolving, business processes change, and so do the risks that a public body faces. When risk management is involved, this is a very important factor to consider and keep in mind.

GUIDELINE 2. - UNDERSTAND THE TYPES OF DIGITAL ASSETS.

Digital assets include a wide range of information and resources that are vital to the operation of a government agency. It is critical to have a thorough awareness of all of the different types of digital assets that exist within the company. Sensitive data, intellectual property, financial information, infrastructure components, communication systems, and other items may be included. Organizations can better prioritise their protection and dedicate appropriate resources for their cybersecurity operations by identifying and categorizing these assets.

GUIDELINE 3. - UNDERSTAND CYBERSECURITY INFRASTRUCTURE AND RESPONSIBILITIES.

There are five basic functions for any cybersecurity infrastructure; Identification, Protection, Detection, Response, and Recovery. This includes everything from threat prevention to security infrastructure design to incident detection and response. It is critical that these responsibilities are carried out correctly because they ensure proper security operations on a daily basis.

GUIDELINE 4. - PROMOTE AGILITY AND ADAPTABILITY.

(1) Keep in mind the changing and dynamic cybersecurity landscape and there should always be room for change. Through strategies, techniques and processes developed, always ensure that they are agile, and changes can be made, and new strategies adapted.

(2) Cybersecurity risks are always evolving, new technologies are introduced every day and business processes often change, therefore ensure that whichever strategy or plan that is developed is agile and adaptable to the constantly changing landscape.

GUIDELINE 5 - USE TOOLS THAT ARE "BEST FIT" FOR YOUR DEPARTMENT OR AGENCY.

There are multiple security solutions, but it is important to remember that the best tools are only effective if they do not leave gaps, and visibility and control can be maintained across all segments.

GUIDELINE 6 .- DEVELOP STRATEGY FOR DEPLOYING.

Updates and patching are critical components of security operations. There should be a strategy in place for regular security updates and patches. After a vulnerability is detected, patches should be made as soon as possible. This is because a network is vulnerable to data theft, malware installation and other types of damage. Patching should always be prioritised and deployed quickly, with full visibility into identified vulnerabilities and what each patch addresses.

GUIDELINE 7. - CONTINUOUS MONITORING OF NETWORK.

Security breaches can happen at any time and therefore it is important that the network should be closely monitored continuously. This ensures rapid detection and response, real-time information on critical processes, and risk management support. This can be done with tools like intrusion detection systems that provide alerts anytime there is suspicious activity.

GUIDELINE 8 . - USE BOTH INTELLIGENT AUTOMATION AND HUMAN RESOURCES TO RESPOND TO THREATS.

Technological advancements continue to improve the accuracy of detection tools and their ability to assess each risk. Organizations can ensure the safety of their network and assets while spending the least amount of time, money, and effort by combining highly skilled security professionals with AI-enabled solutions. Such Artificial intelligence such as;

- *Sophos Intercept X. ...*
- *Symantec Endpoint Security. ...*
- *Splunk User Behavior Analytics. ...*
- *Vectra Threat Detection and Response. ...*
- *IBM QRadar Advisor With Watson*

PART VIII. - INCIDENT RESPONSE GUIDELINES AND BEST PRACTICES.

16. OVERVIEW.

(1) This Part describes guidelines and best practices for developing incident response policies (refer to Standard 3 Internal Security Policy) and plans for public bodies.

(2) These guidelines are largely based on international best practices as well as NCSCs Cyber Incident Management Arrangements (CIMA). Having regard to these guidelines, each public body may document its own incident response policies.

GUIDELINE 1. - KNOW DIFFERENT PHASES OF INCIDENT RESPONSE.

(1) It is important to know the different phases of incident responses. NIST SP 800-61 offers a definition of six phases for incident responses: Preparation, Detection, Containment, Investigation, Remediation and Recovery (Computer Security Incident Handling Guide). The figure below highlights these stages.

FIGURE 5 – PHASES OF INCIDENT RESPONSE.

PHASES OF INCIDENT RESPONSE		
	Phase	**Description**
1	Preparation	Preparation starts with the policies, standards, plans and strategies that every public body has in place. This includes: (*a*) Implementing various controls for responding to \ security incidents within the public body. (*b*) Developing "contingency plans" for incidents that make it unsafe for staff, interrupt/damage communications, network, services, or equipment, or for example, incidents in remote sites. (*c*) Creating a communication channel between relevant security departments, agencies, or offices so that the public body has contacts or aid in the event of an incident. (*d*) Training and awareness within public bodies so that staff are alert and mindful of the ever-changing cybersecurity posture. This ensures that they know different types of cyberattacks and what ransomware/malware can do, enabling them to be safe online.

2	Detection	This phase describes how to identify "unusual behavior", through automated security tools, or monitoring of the network, and to determine its cause, and assess and assign a severity level to it. According to NCSC, there are four levels of severity, called threat condition levels: (*a*) Normal (Green status) – no expected cyber-attack to occur. (*b*) Elevated (Yellow status) – public bodies are warned to take precautions, i.e., possible cyberattack to occur. (*c*) High (Orange status) – a high possibility of cyberattacks, hence, public bodies should prepare to defend against such an attack. Attack should impact the organization. (*d*) Critical (Red status) – cyberattack on a public body in progress. High and significant impact on the organisation. Too often, the detection and assessment of an incident is the most challenging aspect of incident response.
3	Containment	This phase depends on the strategy that is used as the right strategy will prevent greater damage to the affected system/service and make investigation easier. This includes - (*a*) Identification of the affected system and choosing a proper containment strategy; (*b*) Risk mitigation; (*c*) Communication with relevant departments/agencies and offices that deal with cybersecurity issues.
4	Investigation	Through investigation, the cause and severity of the incident is determined. This involves the following: (*a*) Gather evidence to resolve the issue but also for legal \ proceedings, through assessments and analysis; (*b*) Identify threat actors (attacking hosts); (*c*) Determine the root cause of the attack and the damage it caused; (*d*) Determine its threat level (severity); (*e*) Identify any ongoing threats.
5	Remediation	Through remediation, solving the underlying problems and putting solutions in place in order to get operations back on track.
6	Recovery	This phase involves restoring affected systems, services and/or devices.

FIGURE 6 - DESCRIPTION OF EACH INCIDENT RESPONSE PHASE.

he phases listed in Figure 6 represent a strategy of identifying, reacting and dealing with a security issue within a public body.

GUIDELINE 2 - CREATE PROPER COMMUNICATION CHANNELS FOR INCIDENT RESPONSE TEAM.

(1) Establish and maintain a relationship and contact with relevant agencies and offices that provide support to cybersecurity issues. It is critical to identify other groups that may need to participate in incident response so that their assistance can be sought before it is required.

(2) These relevant organizations include the following:

(*a*) Department of Information and Communication Technology (DICT); and
(*b*) Office of Security Coordination and Assessment (OSCA); and
(*c*) National Information and Communication Technology Authority (NICTA); and
(*d*) PNG Computer Emergency Response Team (PNGCERT); and
(*e*) National Cybersecurity Center (NCSC); and
(*f*) Royal Papua New Guinea Constabulary (RPNGC).

GUIDELINE 3 – KNOW WHAT TO REPORT.

(1) Properly report on the incident by including important, however small, details about what occurred.

(2) Details of the following may be included:

(*a*) the time and date of the incident; and
(*b*) the location of the incident; and
(*c*) a concise and complete description of the incident, including the type of incident and how it was detected; and
(*d*) the impact or damage on affected areas of the organization; and
(*e*) the investigation results, including graphic media (i.e., images or surveillance footage) of the incident; and
(*f*) the remediation and recovery process; and
(*g*) recommendations for future steps.

(3) The primary reason for investigating incidents is to identify the root cause(s) that contributed to the incident, so that there is a better chance of preventing the same type of incident from occurring again.

(4) Determining the facts of the incident will also aid in the identification of control measures that can be implemented in the future.

GUIDELINE 4 - DOCUMENTATION, TRACKING AND REPORTING.

Keep track of all the details of the incident and document it properly. This ensures proper reporting of the cybersecurity breach and can be used to develop new strategies to prevent this type of incident from happening again.

GUIDELINE 5 - TRANSPARENCY WITH USERS.

(1) When users experience a service disruption, the incident is usually made public quickly. It is important to publicly acknowledge that there is a disruption and assure users that there are steps being taken to resolve the issue.

(2) It is also critical to communicate the outcome of any incident investigation to employees, so that they are all aware of potential risks and changes made by the organisation to a process or procedure, as well as the reasons for those changes.

GUIDELINE 6 - MONITORING AND EVALUATION.

Compliance assessments and cybersecurity audits will need to be conducted to ensure that public bodies are following the standards framework. These assessments will identify the cybersecurity risks, potential threats, and vulnerabilities that each public body has, as well as the policies, processes, and rules in place to mitigate those risks.

GUIDELINE 7 - BUILDING CYBERSECURITY MONITORING AND EVALUATION.

(1) One of the goals of cybersecurity is to continuously build cybersecurity resilience. Cyber resilience is the ability to enable business acceleration by preparing, responding to, and recovering from cyber threats. A public body that is cyber-resilient can adapt to known and unknown crises, threats, adversities, and challenges.

(2) All public bodies must maintain such resiliency. All public bodies must be more resilient than ever before to cyberattacks. This is not just to protect government functions and public services but also to realize the ambitions set out by the National Cybersecurity Centre (NCSC).

PART IX. - MISCELLANEOUS.

17. IMPLEMENTATION SCHEDULE.

(1) The Cybersecurity Standards and Guidelines is effective from [01.07. 2023].

(2) All public bodies must meet the mandatory standards in Parts 2, 3 and 4 on or before [01.07.2024].

(3) All public bodies must meet the requirements presented in this instrument on or before [01.12.2024].

18. COMPLIANCE AND MONITORING.

(1) To ensure effective compliance of this document, compliance assessments and cybersecurity audits will be conducted to ensure that public bodies are following these standards.

(2) These assessments will identify the cybersecurity risks, potential threats, and vulnerabilities that each public body has policies, processes, and regulations in place to mitigate those risks.

(3) It is also important to note that software license including other licenses all relating to this document will be closely monitored and assessed. This includes monitoring of cracked or unlicensed software used by any public body.

(4) Upon request by DICT, each public body must -

(*a*) conduct an internal self-assessment and prepare evaluation report on its compliance with these Standards; and

(*b*) submit the evaluation report to DICT on its assessment findings and an action plan regarding any areas of non-compliance on how and when it intends to comply fully with these Standards.

Appendix C provides a checklist for what a cybersecurity audit consists of.

19. SUPPLEMENTAL STANDARDS AND GUIDELINES.
DICT may issue supplemental standards and guidelines to support this instrument.

Appendices.

APPENDIX A (INFORMATIVE) – REFERENCE TO PROCUREMENT **GUIDELINES**

The RFP issued to vendors should include the security requirements of the standard for the applicable domains such as:

(*a*) Network architecture security

(*b*) Removal of unnecessary services and programs

(*c*) Antimalware and host-based intrusion protection and prevention

(*d*) Filesystem and O.S hardening

(*e*) Patching mechanisms including 3rd party patching

(*f*) Firewalls/IPS/IDS implementations

(*g*) Changing default accounts and role-based access

(*h*) Password management

(*i*) Logging infrastructure

(*j*) Backup and restore procedures.

More supporting information can be found in the (Cyber Security Procurement Language for Control Systems) issued by ICS-CERT, 2009.

- http://ics-cert.us-cert.gov/pdf/FINAL-Procurement_Language_Rev4_100809.pdf Where it further defines the following:

Topic Basis: A topic's basis is a summary of the potential exposures and vulnerabilities associated with a particular class of problem, that is, why the topic is included.

Procurement Language: Terminology as explained in section 14 of the document (Cyber Security Procurement Language for Control Systems).

Factory Acceptance Test Measures: The Factory Acceptance Test (**FAT**) is necessary to ensure security features function properly and provide the expected levels of functionality. Each topic in the RFP should include factory acceptance test tasks specific to that topic. Note that FAT is a process, not an event, and could in fact extend over several weeks or months.

Site Acceptance Test Measures: The asset owner's Site Acceptance Test (**SAT**) typically repeats a subset of a FAT after system installation, but before cutover or commissioning, to demonstrate that the site installation is equivalent to the system tested at the Vendor's factory or as described in the Systems Manuals. Like the FAT, the SAT may extend several weeks or months and in addition occur at multiple locations.

Maintenance Guidance: This is guidance on how the vendor will maintain the level of system security established during the SAT as the system evolves, is upgraded, and patched. This subsection may be best included as a security clause in a maintenance contract, rather than in a procurement specification to maintain on-going support.

APPENDIX B (NORMATIVE) - APPROVED CRYPTOGRAPHIC ALGORITHMS AND PROTOCOLS
Symmetric Key/Private Key:

Cryptographic functions that use a symmetric key cipher (sometimes referred to as private key encryption) employing a shared secret key must adopt one or more of the following specifications.

Algorithm Name	References	Approved Use	Required Key Length
AES	Advanced Encryption Standard block cipher based on the "Rijndael" algorithm [AES]	General Data Encryption	256-bit keys
TDES /3DES	Triple Data Encryption Standard (or Triple DES) block cipher [SP800-67]	General Data Encryption	three unique 56-bit keys
Note: AES should be used unless this is not technically possible. TDES usage should be limited to systems not supporting AES.			

Asymmetric Key/Public Key:

Cryptographic functions that use *asymmetric key ciphers* (also known as public key encryption) that employ a pair of cryptographic keys consisting of one public key and one private key must adhere to the following specifications:

Algorithm Name	References	Approved Use	Required Key Length
RSA	"Rivest-Shamir-Adleman" algorithm for public-key cryptography [RSA]	Digital Signatures, Transport of encryption session keys	1024-bit keys
DSA	Digital Signature Algorithm [FIP186-2]	Digital Signatures	1024-bit keys

Hashing algorithms

Secure hash algorithms can be used to support implementation of keyed-hash message authentication Generally, Hash functions are used to speed up data comparison tasks — such as finding items in a database, detecting duplicated or similar records in a large file or system.

Algorithm Name	References	Approved Use	Required Key Length
SHA-n	A secure hash algorithm that produces a hash size of "n" e.g.: (SHA 224, 256 ,384,512) [SHA]	All hashing purposes	n ≥ 256
MD5	Message Digest v5 [RFC 1321]	All hashing purposes	The typical 128-bit state
Note: SHAn SHOULD be used unless this is not technically possible. MD5 usage should be limited to systems not supporting SHA family.			

APPENDIX C CYBERSECURITY AUDIT CHECKLIST.

The following table acts as a guideline of how and what cybersecurity audits consist of -

	Details
Security Solutions	
Internet Service Providers	Refer to Standard 2 for the verified and recommended security solutions
Endpoint Protection	
Firewalls	
Operating Systems	
Intrusion Detection Systems	
Policies	
Security Policies	Refer to Standard 3 for required security policies.
Security	
Information Security	
Network Security	
Email Security	
Other testing and assessments	
Updates and Patching	
Application Control	
Password Access	
Multifactor Authentication	
Backups and Restoration	
Vulnerability Assessments	