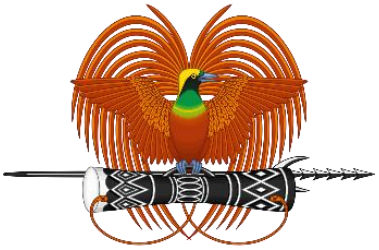

Papua New Guinea

Department of Information and Communication Technology

Cybersecurity Standards and Guidelines

Document Control:

Document Name	Cybersecurity Standards, and Guidelines
Custodian	Department of Information and Communication Technology
Edition	Draft
Approved By	National ICT Sector Coordination Committee
Date Approved	
Effective Date	
Next Review Date	

Table of Contents

Part 1 - Preliminary

1. Name

This instrument is the Cybersecurity Standards and Guidelines 2023.

2. Commencement

This instrument commences on [1 July 2023].

3. Authority

(1) This instrument is made under the Digital Government Act 2022.

(2) This instrument has been produced by the Department of Information and Communication Technology.

(3) The National Cybersecurity Centre will oversee and regulate this instrument.

4. Simplified Outline

(1) This instrument prescribes the standards and guidelines for national cybersecurity. All public bodies must comply with this instrument.

(2) The standards set out are in 2, 3 and 4 in this instrument are mandatory and the standards set out in Part 5 and 6 are not. The guidelines set out in Part 7 are recommended. Part 8 contains other relevant matters and appendices are also part of this instrument.

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

5. Definitions

The defined terms used in this instrument are set out in Appendix 1.

6. Objects of Standards and Guidelines

The objects of these standards and guidelines are to:

(a) achieve a common security "set-up" across all public bodies; and

(b) facilitate a safe and secure digital space; and

(c) effectively manage and mitigate cybersecurity risks; and

(c) increase the security of critical infrastructures, networks, and information technology (IT) systems, thereby improving cybersecurity posture; and

(d) continuingly build resilience in cybersecurity throughout the public sector.

7. Scope and Application

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

(2) This instrument must be read in conjunction with the National Cybersecurity Policy.

(3) Although, these standards should not be limited to a single industry or sector:

(a) All public bodies must adopt this cybersecurity standards.
(b) Non-public bodies may choose to adopt this cybersecurity standards

(4) As stated in (3), only bodies established by an Act of Parliament or government regulation in the PNG Government as a department or agency; a local government entity; a statutory authority; or other defined government body must apply this instrument to their cybersecurity posture and strategy.

8. National Cybersecurity

(1) All public bodies must adopt and apply these mandatory cybersecurity standards in the following parts:

(a) Critical Infrastructure Standards: This standard describes the common basic infrastructure that all public bodies should incorporate into their cybersecurity infrastructure.

(b) Security Solutions Standards: This standard describes standards for security solutions that should be adopted by all public bodies.

(c) Internal Security Policy Standards: This standard provides standards for internal security policies created and implemented by public bodies.

(2) Public bodies may choose to adopt and apply these cybersecurity standards and guidelines in the following parts:

(a) Risk Management Standards: This standard provides the best practices for risk management in the government.

(b) Governance Standards: This standard provides best practices for governance in cybersecurity.

(c) Cybersecurity Operational Guidelines: This section 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.

(d) Incident Response Best Practices: This section provides a guideline for Incident Response Polices and strategies based on best practices as well as the existing NCSCs CIMA.

(3) Public bodies must comply with the National Cybersecurity Policy as well as Papua New Guinea Digital Transformation Policy.

9. National Cybersecurity Centre

(1) The National Cybersecurity Centre (NCSC) is responsible for national cybersecurity.

(2) The Department of Information and Communication Technology is responsible for the administration and management of NCSC.

(3) NCSC will deal with all matters relating to national cybersecurity.

10. National Cybersecurity Policy

(1) The National Cybersecurity Policy (available on the Departments' website) states that the development of cybersecurity standards can assist in the establishment of common security requirements and the necessary security solutions. This policy recognizes that Papua New Guinea has entered the "digital age," which brings with it increased cybersecurity risks. As a result, it is critical that this country strengthens its cybersecurity resilience.

(2) This is supported by the Digital Transformation Policy, which emphasizes on the need to promote and foster a "safe, and secure digital space". Additionally, the National Security Strategy, which was issued in 2013 clearly aims to support the government in making decisions and addresses the numerous security concerns the country is currently experiencing.

(3)The National Cybersecurity Policy additionally highlights the need for cybersecurity standards. The primary goal of such standards is to define "common security requirements and capabilities required for secure solutions". These standards should be based on international best practices.

Part 2 - Critical Infrastructure Standards

11. Overview

(1) Part 2 sets out the Critical Infrastructure Standards. These standards establish a security baseline that specifies the minimum controls that must be implemented or addressed in any critical ICS system.

(2) Critical infrastructure organizations that rely on Industrial Control Systems (ICS) have begun to incorporate commercial-off-the-shelf (COTS) technology developed for business systems into their daily operations. This has provided an increased opportunity for cyber-attacks against the critical systems they operate. These COTS systems are not usually as robust at dealing with cyber-attacks as these systems are designed specifically for Critical Infrastructure at dealing with cyber-attack for many reasons. These

weaknesses may lead to health, safety and environmental (HSE), or operational consequences that can severely affect the Papua New Guineas' economy, people, or its government.

(3) The objects of the Critical Infrastructure Standards are to:

(a) establish a consistent security set-up across all public bodies.

(b) increase the protection of essential systems and services.

(c) facilitate an efficient manner of developing intelligence to drive security strategy and policy.

(3) The following standards must be used as a security minimum by all public bodies and should be used in conjunction with a risk-based security management approach.

(4) These standards are mandatory.

Standard 1.1 Security Policy Standard

The following standards give public bodies that use ICS components direction for creating "defense-in-depth" strategies. Information on secure configuration, best practices, security policy, safe network architecture, and secure operating procedures is provided by this standard. The objective of this is to provide management direction, approval, and support for ICS security in accordance with business requirements and relevant laws and regulations.

1.11 Security Policy	A public body security policy document must be approved by senior management, published, and communicated to all employees and relevant external parties either as part of the public body information security policy or as a separate policy.
1.12 Security Program Leadership	The senior management responsible for public body security must be identified by name, title, business phone, business address and date of designation. Changes to the senior management must be documented within thirty (30) calendar days of the effective date.
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 Procurement Process Standard

This standard is 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 B.
1.22 System Acceptance	Acceptance criteria for new systems, upgrades, and new versions must be established in accordance with the 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 controls in this document.
1.23 Outsourcing contracts	The security requirements of a public body that outsources the administration and/or control of all/some of its systems, networks, and desktop environment must be addressed in a contract agreed upon by both parties. The public body must ensure that the third-party service delivery agreement or contract includes the baseline controls outlined in this document. This must also apply to the third party's subcontractors.

Standard 1.3 Public Body Security Standards

The following set of standards provides recommendations that a public body imposes on its operations in order to safeguard sensitive data. The objective of this is to have a well-defined organizational security when managing public bodies systems.

1.31 Incorporating Security	Management must incorporate the management of the public body security within the organizational governance/ security scheme or security program and explicitly acknowledge their public bodies security responsibilities.
1.32 Change Management	The public body must establish dedicated public bodies change management committee that reviews and approves proposed changes.

	This committee must have representation from corporate IT amongst other as necessary.
1.33 Security Coordination	Public body security activities must be coordinated by representatives from different parts of the public body with relevant roles and job functions, e.g., Physical security, Emergency Response, Corporate IT, etc.
1.34 Allocation of Responsibilities	All public body responsibilities must be clearly defined.
1.35 Authorization process	A management authorization process for new public body information processing facilities must be defined and implemented.
1.36 Confidentiality Agreements	Requirements for confidentiality or non-disclosure agreements reflecting the public body needs for the protection of the public bodies Information must be identified and regularly reviewed, either as part of the contract renewal process or when seen 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 Standards

These standards ensure that the assets and resources are protected from tampering, damage, theft, or illegal physical access through physical and environmental controls. The objective of this is to prevent unauthorized physical access, damage and interference to the premises, equipment, and information.

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 contains public body processing facilities.

1.42 Communication Medium	Extra/separate physical protections must be in place to protect distribution/communication lines from accidental damage, tampering, eavesdropping or in transit modification of unencrypted communications. Protective measures include locked wiring closets/ manholes, protected cabling duct or trays, etc.
1.43 Display Medium	Controls for the physical access to devices that display public body information must be in place. See 1.32
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 authorized or they are owned, provisioned, and audited by the public body.

Standard 1.5 Communication and Operations Management Standards

These standards ensure that information processing facilities are operating properly and securely. This objective of this is to ensure the correct and secure operation of information processing facilities.

1.51 Operational Procedures and Responsibilities

Documented Operating Procedures	Public bodies operating procedures must be documented, maintained, and made available to all authorized users who need them. Vendors must supply the public body with the full documentation for any operating procedure required on their systems.
Change in Management	Changes to public body information processing facilities and systems must be controlled and pre-approved by the dedicated public bodies change management committee. See 1.32
Operational Facilities	Development, test and operational facilities must be physically separated to reduce the risks of unauthorized or inadvertent access or changes to operational systems.

1.52 Third-Party Service Delivery Management

Service Delivery	Public bodies must ensure that the security controls, service definitions and delivery levels included in third party service delivery agreement are implemented, operated, and maintained by the third party in accordance with the terms and conditions set forth in the contract.
Monitoring and Review	The services, reports and records provided by the third party must be regularly monitored and reviewed, and audits must be carried out regularly.
Management of Changes	Changes to the provision of services, including maintaining and improving existing public bodies security policies, procedures, and controls, must be managed, taking account of the criticality of systems and processes involved and re-assessment of consequent risks.

1.53 Patching and Protection Against Malicious and Mobile Code

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 whitelists of preapproved processes, etc.
Anti-malware deployments	The public bodies Anti-malware solution must be regularly updated with the public bodies vendor latest published and approved malware definitions or signatures; whenever possible the public body environment should utilize a different Anti-malware product that the one used on the corporate LAN.
Control against mobile code	Where the use of mobile code[1] is authorized, the configuration must ensure that the authorized mobile code operates according to

	a clearly defined security policy, and unauthorized mobile code must be prevented from executing.
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: ▸ The responsible entity must document the assessment of security patches and upgrades "for applicability" within fifteen (30) calendar days of availability of the patch or upgrade from the vendor. ▸ The responsible entity must document the implementation of vendor approved security patches. In any case where the approved patch is not installed, the responsible entity must document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk. Internal procedures for applying critical/urgent patches or compensating controls must be developed in case the vendor cannot deploy critical patches in a timely manner.
Technical Vulnerabilities	Timely information about 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] Scripts like JavaScript and VBScript, Java applets, ActiveX controls and macros embedded within office documents, etc.

1.54 Backup

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.
Offsite Backup	At minimum, annual backups, or as changes occur backups must be stored offsite 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.
Equipment	The public body must ensure the availability of critical equipment backup components and spare parts.

1.55 Network Security and its Management

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 bodies network, including information in transit.
Security of network services	Security features, service level agreements, and management requirements of all network services must be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
Network Architecture	Public bodies must utilize a three-tier network architecture (as a minimum) which include each of the following components in a physically/logically separate tier: ▸ Corporate/Enterprise LAN ▸ Public bodies (DICT) Shared DMZ ▸ Public bodies network ▸ 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.
Direct Connection	Internet connections must not terminate directly into the public body network. In case of a time limited, continuously monitored and approved exception a firewall must be used to isolate the network from the Internet.
Inbound and Outbound Connections	Firewalls must be used to segregate corporate networks from control networks. The firewall base rule must be "*deny all, allow explicitly*". Inbound connections to the public body 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 firewall must be limited to essential communications only. All outbound traffic from the public body to the corporate network must be source and destination restricted by service and port using static firewall rules.
Intrusion Detection and Prevention	An IDS/IPS solution must be implemented at the Public body DMZ level to detect possible intrusions from the corporate network, the public body should also deploy IDS/IPS within the Public body network if technically supported.
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 from the corporate LAN or 3rd party networks. Traffic must, additionally be restricted by IP address to specific management/support stations. Logs generated from remote connections must be kept for a period of not less than 90 days

	"where technically possible". As per section 1.58
Wireless Devices	Wireless devices should be avoided in critical systems. Where this is not possible, the public body must use authentication and cryptography for enhanced security mechanisms (at least utilizing WPA encryption for 802.11x networks) to prevent unauthorized wireless access into the system. Public bodies 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.
Network Traffic	The allowed types (protocols/ports/applications) of the traffic must be defined, approved, and documented.
Monitoring of Network Traffic	Public bodies must "continuously" monitor and retain the public body network (Layer 3 and 4) logs as a minimum for a period of not less than 90 days. In addition, should ensure that the logs are centrally stored and managed. As per section 6.9.
Industrial Protocols	Public body's related protocols such as (MODBUS/TCP, EtherNet/IP and DNP3) MUST only be allowed within the Public body networks and not allowed to cross into the corporate network without explicit management approval.
WirelessHART Communication	The WirelessHART network must meet the following security controls: - Ensure no interference on the allocated band spectrum. - The security manager is connected directly through a dedicated connection to the network manager. - The network gateway firewall default configuration is "reject all." - Individual session keys for devices

	- All devices pre-configured with the "join key." - Ensure the whitelisting - access control list (ACL) includes the individual keys and the globally unique HART address AES-128 encryption as a minimum.
ZigBee Wireless Communication	The ZigBee network must meet the following security controls: - Network Infrastructure is protected with a network key. - Encryption security service is enabled. - Filtering done via MAC addresses. Source node authentication enabled.
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 network to collect the data from the control / RTUs and a second server on the corporate network mirroring the first server and supporting client queries.
Dial-Up Modems	Public body must limit the use of dial-up modems connected to the public body networks. Where other alternatives are not possible, the following controls must be in place: ▸ Call back features. ▸ Default passwords must be changed. ▸ Physically identify the modems in use to the control room operators. And make sure they are counted and registered in the approved HW inventory. ▸ Disconnect the modems when not in use or setup them up to automatically disconnect after being idle for a given period of times. If modems are used for remote support, make sure these guidelines are well communicated to the support personnel.

Equipment Identification	Automatic equipment identification solutions (based on MAC address filtering as an example) at layers 3 and 4 MUST be used as a mean to authenticate connections from specific locations and equipment. In addition, to detect rouge connections and devices.
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.
Segregation of Networks	Information services, users, and information systems must be segregated on networks.
Segregation of Duties	Segregation of duties for public body security operating personnel must be followed.
Network Connection Control	For shared networks, especially those extending across the public body physical boundaries, the capability of users to connect to the network must be denied. Named exceptions must be in line with the access control policy.
Data Diodes/ Unidirectional Gateways	Systems should utilize the Data Diode / Unidirectional gateway technologies for additional security whenever only one-way communication is required and technically feasible.
Firewall Deployment	Public bodies should utilize a different Firewall product than the one used on the corporate LAN, if supported by ICT vendor.
1.56 Media Handling	
Management of Removable Media	Removable media (such as USB/CD/DVD) must not be allowed into the public body control room or used within the system unless explicitly authorized by management. The removable media ports/drivers must be blocked by default. Where allowed removable media

	MUST be scanned prior use and/or restricted to a pool of sanitized media.
Disposal of Media	Media must be disposed when no longer required, using the public body's formal procedures for safe and secure information sensitization.
Information Handling Procedures	Procedures for the handling and storage of public body information must be established to protect this information from unauthorized disclosure or misuse.
Security of System Documentation	Public body System documentation must be protected against unauthorized access or unauthorized disclosure.

1.57 Exchange of Information

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.).
Exchange Agreements	Agreements (Such as Non-Disclosure Agreements –NDA) must be established prior exchanging public body information or data (in any form) between the public body and external parties.
Physical Media in Transit	Media containing public body's information must be protected against unauthorized access (e.g., by using encryption), misuse or corruption during transportation beyond an public body's physical boundaries. Details of acceptable encryption protocols/keys are specified in Appendix A.
Electronic Messaging	Public body information sent via electronic messaging must be appropriately protected by means of Encryption as an example.

1.58 Monitoring

Audit Logging	Audit logs, exceptions, and information security events where technically possible, must be produced and kept for ninety (90) calendar days to assist in access control/authorization monitoring and to support any investigations.
Central Logging	Logs should be kept and managed centrally on a dedicated logging infrastructure.
Monitoring System Use	Procedures for regularly monitoring use of Public body information processing facilities must be established and the results of the monitoring activities reviewed regularly, handled or escalated as per the established procedures.
Protection of Log Information	Logging facilities and log information must be protected against tampering and unauthorized access. Public body's logs must be stored both physically and logically separate from corporate IT logs.
Administrator and Operator Logs	Public body administrators and operators' system access activities must be logged.
Fault Logging	Faults must be logged, analyzed, and appropriate action taken.
Clock Synchronization	The clocks of all critical public body systems within an public body must be synchronized with an accurate (UTC or GMT+3) time source.

Standard 1.6 Access Control Standards

This standard defines the controls that limit access to government information and assets. The objective of this is to control access to systems and information and ensure the availability of access control logs and functionality of the overall process.

1.61 Access Policy and User Access Management

Access Control Policy	A public body 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 privilege* and *personal/named accountability* concepts.

	Account management may include additional account types (e.g., role-based, device-based, attribute-based).
User Registration	There must be a formal public body 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).
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.
User Password Management	The allocation of passwords must be controlled through a formal management process.
Password Complexity	For critical public body systems and as technically feasible, The public body must require and use passwords subject to the following: ▸ Each password/pass phrase must be a minimum of twelve characters. Each password must be changed at least annually, or more frequently based on the adopted risk assessment.
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.
Testing	The responsible entity 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

Network Services Usage	Users must only be provided with access to the public body's services that they have been specifically authorized to use.
Secure Log-On Procedures	Access to public body systems must be controlled by a secure log-on procedure in line with the public body's access control policy.
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 personal/named identification[2], the following must be maintained: ▸ A recorded, valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria. ▸ Compensating controls for automated user identification such as CCTV, Smart cards…etc. ▸ The public body specifically authorizes and monitors the use of guest/shared/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. ▸ The public body removes, changes, disables, or otherwise secures default accounts. ▸ Account/shift managers are notified when users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. ▸ Account/shift managers are also notified when users usage or need-to-know/need-to-share changes. ▸ 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.

Password Management Systems	Systems for managing/storing public body passwords must be interactive and must ensure and enforce strong passwords.
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.
Session Time-Out	Inactive public body sessions must shut down automatically after a defined period of inactivity.
Concurrent Session Control	Public bodies systems must limit the number of concurrent sessions for any given user and/or username in line with the public body's policy on concurrent sessions.
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 defined as per the public body risk assessment process.

1.63 Field Device Access and Remote Terminal Units (RTU)

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 physical security perimeter but must be enclosed and monitored within the electronic security perimeter.

RTUs with Routable Protocols	Devices such as RTUs that use routable protocols must be enclosed within the entity's physical security perimeter as well as the electronic security perimeter.
Authenticating RTUs	Secured field devices should use cryptographic certificates issued/trusted by a plant certificate authority to ensure device identity.
Direct Access to Field Devices	Any direct access to operational field devices that is made by field personnel should be provided in such a way that there are permission checks applied to that access. Including 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.
RTUs Access Logging	Secured field devices should 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.
RTU Communication Interface	Communication links to RTUs should be encrypted as specified in Appendix A. Encryption implemented on the communication interface should 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 standard ensures that proper identification and management of security threats or incidents. The objective of this is to ensure information security events and weaknesses associated with public body information systems are communicated in a manner allowing timely corrective action to be taken.

1.71 Incident Response Policy	The responsible entity must develop and maintain an public body information security incident response plan to address at a

minimum, the following:

- Procedures to characterize and classify events as reportable security incidents.
- Procedures to properly and in a timely manner report security incidents to the appropriate management channels
- Process for updating the incident response plan within thirty (30) calendar days for any changes in the reporting mechanism, organizational hierarchy, contacts, etc.
- 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 requirement in their contracts, job descriptions, etc.

1.73 Contacting the Authorities

The responsible entity must establish communication contacts as applicable with the national C-CERT (NCSC) for reporting incidents of criticality level one (as identified in the NIA Appendix C.) and the applicable critical infrastructure protection laws.

Standard 1.8 Business Continuity Management

These standards describe how to maintain business continuity after an incident or disaster has occurred. The objective of this policy is to counteract interruptions to business activities, to protect critical public body processes from the effects of major failures of information systems, network disruptions or disasters, and to ensure their timely resumption.

1.81 Business Continuity & Disaster Recovery

The public body Business Continuity Plan (BCP) must be a component within the corporate BCP and must include the following items as a minimum:

- Business impact classification and prioritization of the public body assets
- Required response to events that would activate the plan.
- Procedures for operating the systems' basic functionalities in a manual mode, until normal operational conditions are restored.
- Roles and responsibilities of the Public body BCP responders
- Complete up to date documentation (manuals, configurations, procedures, vendors contact lists, network diagrams...etc.)
- Personnel list for authorized physical and logical access to the systems.
- System components restoration order/sequence
- Offsite backups recall and restoration procedures.
- Procedures for liaison with the appropriate authorities as per the public body BCP.

Standard 1.9 Compliance

The following standards describes compliance control that must be tested against a set of IT infrastructure to determine compliance. A public body is required to abide by any rules or specifications imposed by the public body itself or by laws.

The objective of this is to avoid breaches of any law, statutory, regulatory, or contractual obligations and to ensure compliance of systems with national and/or organizational security current or future policies and standards. It also covers system audit considerations.

1.91 Compliance

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.
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.
Technical compliance	Public body systems must be regularly self-checked for compliance with security implementation standards, or guidelines including this document, at least annually.
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.
Levels of Non-Compliance the following schedule:	Audit findings require rectification in line with ▸ Level 1: minor non-conformities and observations must be rectified within six (6) months. ▸ Level 2: major non-conformities must be rectified within three (3) months and acknowledged by the senior management.

1.92 System Audit

Information System Audit Controls	Audit requirements and activities involving checks on public body operational systems must be carefully planned and agreed to minimize the risk of disruptions to business operations.
Protection of Audit Tools	Access to public body information systems audit tools must be protected to prevent any possible misuse or compromise.

Standard 1.10 System Hardening

The objective of this standard is to ensure unused services in a host operating system (OS)/public body system are disabled. Only services used by the system, its operation and maintenance should be enabled to limit possible entry points or vulnerabilities.

Vendor Application Whitelist	Public body must obtain and maintain a list of all applications, utilities, system services, scripts and all other software required to keep the system operational (I.e. High risk assets).
Software/Services to be Removed	All unnecessary software/services must be removed; this includes but not limited to: ▸ Games ▸ Device drivers for hardware not included. ▸ Messaging services ▸ Servers or clients for unused internet or remote access services ▸ Software compilers (except from non-production, development machines) ▸ Software compliers for unused languages ▸ Unused protocols and services ▸ Unused administrative utilities, diagnostics, network management and system management functions ▸ Test and sample programs or scripts ▸ Unused productivity suites and word processing utilities for example: Microsoft word, excel, PowerPoint, adobe acrobat, open office, etc. ▸ Unlicensed tools and sharewares ▸ Universal Plug and Play services.
Restricting Bluetooth Access	Bluetooth wireless access technology must be denied by default.
BIOS Protection	The BIOS (Basic Input/Output System) must be password protected from unauthorized changes.

Disabling Well Known/Guest Accounts	Default accounts and passwords must be disabled or changed to meet the public body complexity requirements, Where not possible due to technical limitations compensating controls must be implemented.
Equipment Certification	Public bodies must ensure that the ICS security devices utilized have achieved EAL (Evaluation assurance level) of 4+ as per the common criteria (ISO 15408).

Part 3 - Security Solutions Standards

12. Overview

(1) Part 3 sets out standards that describes the criteria for security solutions that should be adopted by all public bodies.

(2) The objects of the Security Solutions Standards are to:

(a) establish a solid basis for securing government information and network protection.

(b) help improve national security by only implementing highly recommended and certified security solutions.

(c) maintain a consistent and standardized approach in the security solutions that are implemented across all public bodies.

(3) These standards are mandatory.

Standard 2.1 Internet Service Providers

(1) All public bodies must select one internet service provider to use.

(2) This internet service provider must be decided upon from the list provided below. The following internet service providers have all been approved and verified by NCSC.

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

(3) It should be noted that the preceding table does not show the order of preference. All of these service providers were subjected to NCSC testing to specific criteria, which included national security, ownership, high availability, and maximum capacity to support NCSC operations. Each of these ISPs' services are NCSC-verified, which means they meet NCSC standards and are a high-quality and well-known service provider in the country.

Standard 2.2 Endpoint Security

(1) Public bodies must deploy an endpoint security system over their network.

(2) An endpoint security system must be selected from one of the following highly recommended solutions.

Figure 2 Recommended 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 EventTracker. EventTracker allows monitoring of both security (threat/unwanted application detection) and operation (web content filtering, addition/removal of endpoints and devices).
			Performance	Provides one of the best rated performance features. Fast, simple, and easy to use.
2	Norton	Norton is one of the leading antivirus solutions for 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 7, 8, 10, 11 • Mac • Linux
			Other features	Antivirus and malware protection, smart firewall, cloud backup, etc.

3	Kaspersky	Kasperskys Endpoint Security is another highly recommended security solution, mostly compatible with Windows OS.	Operating System Compatibility	• Windows 7, 8, 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.

(3) All public bodies must collaborate with other security technologies to provide administrators with visibility into advanced threats, allowing them to respond faster to detection and remediation.

(4) An additional solution is Microsoft Defender as it comes with Windows operating system. This is, in addition, one of the best ranked endpoint protection.

Standard 2.3 Firewalls

(1) Public bodies must deploy a firewall over their network.

(2) This firewall solution must be selected from one of the following highly recommended solutions.

Figure 3 Recommended Firewalls

FIREWALLS		
	Firewall	**Description -Features/Additional Details**
1	Sophos	Sophos has the best user interface and one of the best performance. Some more 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	One of the best rated firewalls in the market right now. Features: • 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 an excellent product with a good number of features that are simple to use and configure. Some of these 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

(3) It is through the use of a firewall that ensure data protection and fosters a safe and secure environment for confidentiality, integrity and availability of data.

(4) It is important that there be a consistent variety of firewalls implemented across the government network.

Standard 2.4 Intrusion Detection Systems

(1) All public bodies should implement an Intrusion Detection System.

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

(3) The primary goal is to ensure 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 Upgrade

(1) All public bodies must install Windows 10 or 11 Operating Systems and always be kept up to date at all times.

Note: Most public bodies do not use the most up-to-date operating system for all network devices, including servers.

(2) Microsoft's support for Windows 7 ended in January 2020 and without no support, devices using Windows 7 are more vulnerable to data theft, more specifically classified government data, if security patches aren't applied on a regular basis.

(3) As a result, all network devices, particularly servers, desktops, and laptops, should have the most recent version of operating system installed.

Standard 2.6 Keep software up to date with the latest versions

(1) All software used should be updated every two years, yearly, or whenever a new version is released.

(2) Updates are released by software vendors to address security issues and improve functionality.

(3) Regularly installing updates addresses these flaws, enhances the protection against loss of money, data, and integrity.

Standard 2.7 Use licensed software products only.

(1) All software used by any public body must have proper licenses.

(2) Cracked software must not be used throughout public bodies. In addition, pirated files frequently contain viruses and spyware that can slow down or completely shut down your systems.

(3) Software licenses provide end users with the right to one or more copies of the software without violating copyrights.

Note: Using or distributing pirated software is a violation of software copyright law.

Part 4 - Internal Security Policy Standards

13. Overview

(1) Part 4 sets out standards for security policies for all public bodies.

(2) The objects of the Security Solutions Standards are to:

(a) create a basis for securing government information and network protection.

(b) determine the procedures and policies that should be followed while utilizing the resources and assets of the public body.

(3) These standards are mandatory.

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.

(2) These security policies must include regulations and procedures for cybersecurity, physical security, and cloud security.

(3) The following table lists all security policies that should be created and their requirements.

Figure 4 Internal security policy

	Security Policy	Description
Cybersecurity		
1	Incident Response Policies	This policy ensures that your public body 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 defines 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 public body from cyber threats and cybercrime.
	Access Control and User Management Policies	This policy defines 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.
3	Acceptable Use Policy	This policy defines is an agreement between two or more parties that specifies all of the rights, privileges, responsibilities, and sanctions associated with a corporate network or the internet.

4	Password Policies	This policy defines the rules and best practices for password creation, and maintenance. These rules include: • guidelines for creating, updating, and protecting access through strong and secure passwords. • password complexity and length requirements. • risks of not following length requirements and password complexities, as well as risks of reusing passwords. • password log outs and maximum retry attempts and outline procedures for logging all unsuccessful login attempts., and etc.
5	Email Policies	This policy defines the rules and best and acceptable practices for email use.
6	Network Security Policies	This policy describes how the security rules are applied throughout the network architecture, lays out the public body's network security environment, establishes criteria for computer network access, and determines policy enforcement.
7	Backup Policies	This policy establishes measures designed to protect data and system backups, and also sets rules for planning, executing, and validating backups. This should also ensure that critical government data is backed up in a secure location. This also includes disaster recovery and file recovery procedures and plans. Refer to Standard 1.54 Backup.
Physical Security		
8	Physical Security Policies	This policy establishes measures that are designed to protect physical locations and the resources and equipment, information, and employees within. This also includes procedures and strategy for standards listed in Standard 1.4 Physical and Environmental Standards, 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.

Note: Most of these policies have been mentioned above in Standard 1 Critical Infrastructure.

(4) A public body may choose whether these policies be documented as separate policies or as a single document with all these policies mentioned.

Standard 3.2 Ensure proper approval and documentation of all security policies

(1) All public bodies must ensure that each of the policies mentioned above are properly documented and are available to all users, i.e., the employees.

(2) All security policies should be approved by senior management.

(3) If any changes are made, approval should also be granted.

Refer to Standard 1.51 Operational Procedures and Responsibilities.

Standard 3.3 Review and upgrade security policies

(1) Public bodies must review and upgrade of policies accordingly, so that are in line with the ever-changing cybersecurity scene.

(2) Review may be done by an independent third-party reviewer.

Part 5 - Risk Management Standards

14. Overview

(1) Part 5 sets out standards for risk management within public bodies. The following standards will specify a set of highly recommended strategic methods that should ensure proper risk management practices within the government.

(2) The object of the Risk Management Standards is to identify, evaluate, reduce, and eliminate risks so that these risks have a lower potential impact on that public bodies.

Standard 4.1 Provide a Risk Management Strategy

(1) This strategy must provide a structured approach to addressing risks and must be adopted by all public bodies. Through a risk management strategy, we can:

(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 public body risk tolerance.

(d) Define processes to 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 public body cybersecurity based on existing and documented risks and vulnerabilities.

(2) By implementing such a strategy, public bodies may reduce the impact of cyberattacks and the harm caused by cyber risks, lower your operating expenses, protect your company's assets and revenue, thus improving the image.

Standard 4.2 Create a team of professionals

(1) A team of cybersecurity professionals that are tasked with cybersecurity operations, or more specifically risk management must be in place.

(2) This ensures that risk mitigation is done by a group of highly skilled engineers and analysts.

Standard 4.3 Develop an incident response policy

(1) An incident response plan must be present and defined in your risk management strategy.

(2) This gives the team instructions on how to handle serious security incident, such as a data breach, ransomware attack, or sensitive information loss.

(3) The four phases of an incident response plan, as published by The National Institute of Standards and Technology (NIST) are (i) preparation, (ii) detection and analysis, containment, eradication, and (iv) recovery, and post-incident activity. All these phases are important in incident responses and should be covered in the plan. Refer to Incident Response Guidelines (Part 7).

Standard 4.4 Review and Upgrade Incident Response Policies and Plans

(1) The incident response plan must always be reviewed bi-annually or annually and are upgraded and consistent with international best practices and the pace at which technology changes.

Standard 4.5 Engage Employees in Risk Management and Cyber Awareness Trainings

(1) All employees in the public sector must undergo risk management and cyber awareness training programs.

(2) Information security policies must be made public, and all employees should be made aware of the cyberthreats. The goal is to raise employee awareness of ongoing security threats (refer to Standards 4 Governance).

Part 6 - Governance in Cybersecurity Standards

15. Overview

(1) Part 6 sets out standards for governance in cybersecurity within public bodies. The following standards will describe the best practices for cybersecurity governance and help in maintaining cyber maturity.

(2) The object of the Governance in Cybersecurity Standards is to define the policies and procedures that govern how public bodies detect, prevent, and respond to cyber-attacks and ensures that the cybersecurity program is aligned with business goals, follows government or industry standards, and meets the leadership's security and risk management objectives.

Standard 4.1 Always assess cybersecurity maturity

(1) Public bodies should always assess its cyber maturity.

(2) Assessing cybersecurity maturity helps to understand which areas are lacking, where improvements need to be made and the risks each public body are facing and where these needs to be remediated.

Standard 4.2 Develop accountability frameworks

(1) Accountability frameworks helps in measuring and monitoring what public bodies are doing and how well it is being done.

(2) Accountability is one of the main data protection principles and this framework will help to deliver appropriate technical and organizational measures that should be taken in respective public bodies .

Standard 4.3 Ensure risks are properly mitigated

(1) The four common risk mitigation processes are avoidance, acceptance, transference, and reduction/control.

(2) Risk mitigation creates a strong culture around risk management (Refer to Standard 3) and prepares the government entity for all potential risks and also ensures or develop plans to prevent completely those risks.

Standard 4.4 Compliance

(1) Ensure compliance in all cybersecurity aspects, including critical infrastructure and security solutions.

(2) In order to manage risks, the process of building and maintaining an IT governance plan ensures that cybersecurity initiatives meet corporate goals and objectives, conform to policies, standards, and internal controls, and assigns authority, roles, and responsibilities.

Standard 4.5 Create/Review/Update policies, standards, frameworks, and procedures and processes.

(1) All standards, regulations and plans should be regularly updated or upgraded accordingly.

Standard 4.6 Increase cybersecurity training and awareness

(1) Create more avenues for employees to be more cyber aware and learn of the different policies, standards, and framework in place.

Part 7 - Cybersecurity Guidelines and Best Practices

16. Overview

(1) Part 7 sets out the guidelines and best practices that all public bodies should take into consideration.

(2) The object of these guidelines and best practices is to improve cybersecurity posture.

Guideline 1: Cybersecurity Operational Guidelines

Cybersecurity operations basically refer to those processes that help identify each public body security capability. The following will act as a guide to illustrate such methods where we can improve cybersecurity operations in the government.

Guideline 1.1 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 the public body faces. When risk management is involved, this is a very important factor to consider and keep in mind of.

Guideline 1.2 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 1.3 Promote agility and adaptability

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

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 landscapes.

Guideline 1.4 Use tools that are “best fit” for your public body

There are multiple security solutions but it is important to remember that the best tools are only effective if they don't leave gaps and you can maintain visibility and control across all segments.

Guideline 1.5 Develop strategy for deploying security updates and patches

Updates and patching are critical component 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 the network is vulnerable to data theft, malware installation and other types of damage. Patching should always be prioritized and deployed quickly, with full visibility into identified vulnerabilities and what each patch addresses.

Guideline 1.6 Continuous Monitoring of Network

Security breaches can happen at any time therefore it is important that there should be the network 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 provides alerts anytime there is suspicious activity.

Guideline 1.7 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.

Public bodies 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.

Guideline 2: Incident Response Guidelines

(1) This section describes the best guidelines to developing incident response policies (refer to Standard 3 Internal Security Policy) and plans for public bodies. These guidelines are largely based on international best practices as well as NCSCs Cyber Incident Management Arrangements (CIMA).

(2) With these recommendations, each public body may document their own incident response policies.

Guideline 2.1 Know Different Phases of Incident Response

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

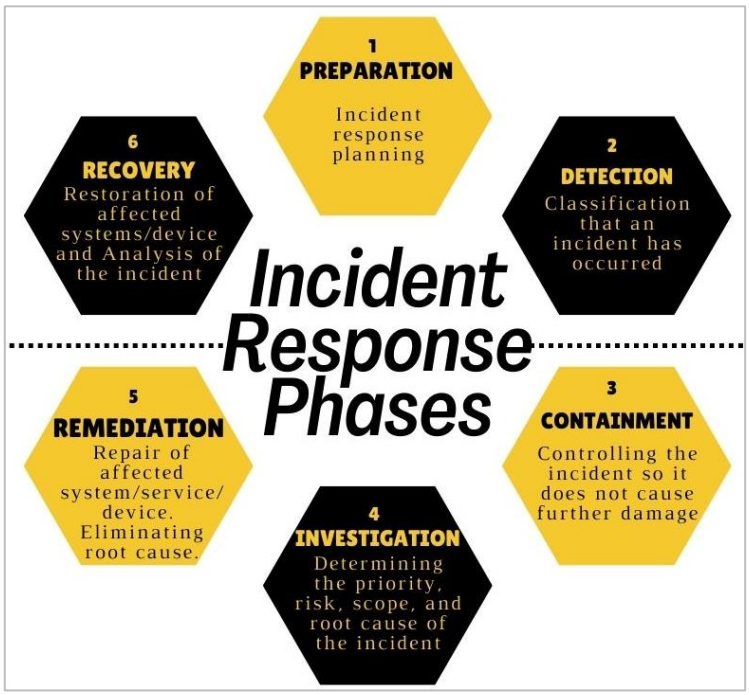

Figure 6 Description of each Incident Response Phase

PHASES OF INCIDENT RESPONSE		
	Phase	**Description**
1	Preparation	Preparation starts with the policies, standards, plans and strategy that every government entity has in place. This includes: • Implementing various controls for responding to security incidents within the government entity. • Developing "contingency plans" for incidents that makes it unsafe for staff, interrupts/damages communications, network, services, or equipment, or for example, incidents in remote sites. • Creating a communication channel between relevant security parties so that the public body has contacts or aid in the event of an incident. • Training and awareness within the public body so employees are alert and mindful of the ever-changing cybersecurity posture. This ensures that they know different types of cyberattacks and what ransomwares/malwares 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, on the network, 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: i) Normal (Green status) – no expected cyber-attack to occur.

		ii) Elevated (Yellow status) – public bodies are warned to take precaution, i.e., possible cyberattack to occur. iii) High (Orange status) – a high possibility of cyberattacks, hence, public bodies should prepare to defend against such an attack. Attack should impact public body. iv) Critical (Red status) – cyberattack on public body in progress. High and significant impact on public body. 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: • Identification of affected system and choosing a proper containment strategy. • Risk mitigation • Communication with relevant parties that deal with cybersecurity issues.
4	Investigation	Through investigation, the cause and severity of the incident is determined. This involves: • Gathering evidence to resolve the issue but also for legal proceedings, through assessments and analysis. • Identify threat actors (attacking hosts) • Determine the root cause of the attack and the damage it caused. • Determine its threat level (severity). • Identify any ongoing threats
5	Remediation	Through remediation, solving the underlying problems and putting solutions in place—so you can get your operations back on track
6	Recovery	This phase involves restoring affected systems, services and/or devices.

The phases as seen above represent a strategy of identifying, reacting, and dealing with a security issue within the public body.

Guideline 2.2 Create proper communication channels for incident response team

Establish and maintain a relationship and contact with relevant parties that provide support to cybersecurity issues. It is critical to identify other groups outside of the public body that may need to participate in incident response so that their assistance can be sought before it is required.

These relevant parties include:

i) PNG Department of Information and Communication Technology

ii) Office of Security Coordination and Assessment (OSCA)

iii) National Information and Communication Technology Authority (NICTA)

iv) PNG Computer Emergency Response Team (PNGCERT)

v) National Cybersecurity Center (NCSC)

vii) Royal Papua New Guinea Constabulary (RPNGC)

Guideline 2.3 Know what to report

Properly report on the incident by including important, however small, detail about what occurred.

You may include details of:

i) The time and date of the incident

ii) Location of the incident

iii) A concise and complete description of the incident, including the type of incident and how it was detected.

iv) Impact/Damage on affected areas of public body

vi) Investigation results, including graphic media (i.e., images or surveillance footage) of incident.

v) Remediation and Recovery process

vii) Recommendations, i.e., future steps

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

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

Guideline 2.4 Documentation, Tracking and Reporting

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

Guideline 2.5 Transparency with users

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.

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

Guideline 3: Building Cybersecurity Resilience

(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) It is very important that all public bodies 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 8 – Miscellaneous

17. Implementation Schedule

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

(2) All public bodies must meet the requirements presented in this instrument on or before [01. 12. 2023].

(3) All public bodies must meet the mandatory standards in Parts 2, 3 and 4 on or before [01.07. 2023].

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, as well as the 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

The Public body may issue supplemental standards and guidelines to support this instrument.

Appendices

APPENDIX 1 - GLOSSARY OF TERMS

TERMS	
anti-malware	a type of software program created to protect information technology (IT) systems and individual computers from malicious software, or malware.
access control	a data security process that enables organizations to manage who is authorized to access corporate data and resources.
cloud	A network of remote servers hosted on the internet and used to store, manage, and process data in place of local servers or personal computers.
compliance	following rules and meeting requirements
critical infrastructure	Critical infrastructure describes the physical and cyber systems and assets that very vital that their incapacity would have a very harmful impact on our physical or economic security or public health or national security.
cyber crime	Crimes directed at computers, such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software. It also includes crimes where computers facilitate an existing offence, such as online fraud.
cyber resilience	The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.
cybersecurity	The state of being safe against the criminal
cyber threat	Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
guideline	A guideline provides general guidance, and additional advice and support for policies, standards, or procedures.
Industrial Control Systems	an electronic control system and associated instrumentation used for industrial process control.
information technology	use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.
intrusion detection system	Any circumstance or event with the potential to harm systems or information.
patching	Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety.
policy	A policy is a formal statement of a principle that should be followed by its intended audience.
procurement	Procurement is the processes used to monitor and improve the cybersecurity of devices, applications, and services as they are acquired and integrated into utility operations, as well as efforts to manage supply chain risk.

standard	something established by authority, custom, or general consent as a model, example, or point of reference. A standard specifies uniform uses of specific technologies or configurations.

Refer to https://www.cyber.gov.au/acsc/view-all-content/glossary and https://csrc.nist.gov/glossary for more terms and definitions

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 any 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 (INFORMATIVE) – REFERENCE TO PROCUREMENT

GUIDELINES

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

- Network architecture security
- Removal of unnecessary services and programs
- Antimalware and host-based intrusion protection and prevention
- Filesystem and O.S hardening
- Patching mechanisms including 3rd party patching
- Firewalls/IPS/IDS implementations
- Changing default accounts and role-based access
- Password management
- Logging infrastructure
- 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 public body 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 D – 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	