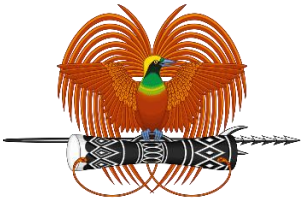

Papua New Guinea

Department of Information and Communication Technology (DICT)

Government Data Standards, Specifications and Guidelines 2025

Document Control:

Document Name	PNG Government Data Standards, Specifications & Guidelines 2025
Prepared by	PNG Department of Information and Communications Technology
Edition	Draft 4
Approved by	
Date Approved	
Effective Date	
Next Review Date	

Table of Contents

Table of Contents

PNG Government Data Standards, Specifications and Guidelines 2025

PART I. PRELIMINARY

1. NAME

This instrument is the PNG Government Data Standards, Specifications and Guidelines 2025.

2. COMMENCEMENT

This instrument commences on the 1st of August 2024

3. AUTHORITY

(1) This instrument is made under Section 64 of the Digital Government Act 2022.

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

4. SIMPLIFIED OUTLINE

(1) This instrument prescribes the standards, guidelines and best practices for all government data. All public bodies must comply with this instrument.

(2) This instrument is set out in 6 parts. Parts 2 and 3 are mandatory, and Part 4, 5 and 6 are recommended. Appendices are also part of this instrument.

(3) Notes are included in this instrument to help understanding by drawing attention to other provisions of 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 this section.

"Central Electronic Data Repository" has the same meaning as the one in Section 28 of the Digital Government Act 2022.
https://www.paclii.org/pg/legis/num_act/dga2022199.pdf

"confidential data" means any data that is not intended for public dissemination.

“data access” has the same meaning as the one in the Digital Government Act 2022.

“data governance” means the management of data availability, accessibility, integrity, and security in corporate systems based on internal data standards and policies that also control data usage.

“government data” refers to any information, document, media, or machine-readable material created or collected by the government, regardless of physical form or features.

“data classification” refers to the process of classifying data into appropriate categories to improve its usability and security.

“data governance” means the process that ensures the effective and secure management of data throughout its lifecycle.

"data infrastructure” refers to the hardware, software, and networking technologies that are used to support the storage, processing, and management of data within a public body.

“data interoperability” means the ability of systems and services that create, exchange and consume data to have clear, shared expectations for the contents, context, and meaning of that data.

“data localization” means the practice of storing and processing data within the jurisdiction to comply with national laws and regulations.

“data protection” means the measures taken to safeguard data from unauthorized access, loss, corruption, or misuse.

“data quality” means the degree to which data in a system is accurate, consistent, reliable, and relevant for a particular use.
“data sharing agreement” means ----------
“data sovereignty” means that data is subject to the laws and regulations of the jurisdiction in which it is collected, processed or stored.

“data subject” means an identified or identifiable living individual to whom personal data relates.
“electronic data” means any data that is stored or transmitted electronically, using computers, networks and other electronic data.

“entities” are organizations apart from public bodies.

“government data” refers to any information, document, media, or machine-readable material created or acquired by the government while conducting official government activity, regardless of physical form or features.

“meta-data” means data that describes and provides context for other data to support its discovery, management, and use.

“open data” means data that is available for everyone to access, use and share.

"personal data" means any data collection that can identify an individual.

"the Department" means the Department of Information and Communications Technology.

"top-secret data" means data that, if disclosed, could cause severe damage to national security or critical infrastructure.

"transparency" means that any information and communication concerning the processing of personal data must be easily accessible and easy to understand

6. OBJECTIVES OF STANDARDS AND GUIDELINES

The objectives of this instrument are to:

(a) establish clear and responsible data governance and data protection practices,
(b) develop and implement protocols for the secure collection, processing, storage, and shaping of data, ensuring that these protocols maintain data consistency, accuracy and completeness while safeguarding against unauthorized access, breaches and data loss.
(c) ensure high data quality, consistency, and interoperability to support seamless integration and efficient information sharing across systems and platforms.
(d) maintain confidentiality, integrity, and availability of data by promoting secure, compliant, and accountable data management practices that align with applicable legal and regulatory requirements.
(e) promote data literacy and awareness.

7. SCOPE AND APPLICATION

(1) This document is developed to provide standards and guidelines for handling government and personal data within both the public and private sectors.

(2) This document covers the following areas and includes;
(a) data management, including the data lifecycle management, and standards that support the integrity, quality, and availability of data.

(b) classification of data, data ownership and sovereignty,

(c) secure data exchange and data sharing,

(d) data security including encryption and controls for safeguarding electronic data against unauthorized use, disclosure, manipulation and destruction,
(e) data privacy, including secure and standardized APIs as mechanisms to facilitate interoperability between and integration of different data platforms and systems,
(f) regulatory and compliance of existing laws, regulations and standards,
(g) data literacy, data awareness, and capacity building.

(2) This document applies to;

(a) all public bodies,

(b) stakeholders doing business with public bodies,

(c) private entities that collect, process and store personal data,

(d) data controllers, processors and data subjects.

(3) All other entities are required to comply with these provisions when interacting with public bodies, including external regulatory bodies or data protection authorities.

8. CENTRAL ELECTRONIC DATA REPOSITORY

(1) The Central Electronic Data Repository (CEDR) is a critical data infrastructure established under Section 28 of the Digital Government Act 2022,

(2) It is designed as a secure, centralized platform for the structured storage, management, and retrieval of high-volume electronic data across public bodies.

(3) CEDR enforces standardized data formats, access protocols, and metadata schemas to ensure data consistency, integrity, and security. By enabling centralized control over data lifecycle processes, including ingestion, classification, access management, and archival, CEDR facilitates interoperability, reduces duplication, and enhances the efficiency and reliability of government data services.

9. NATIONAL DATA GOVERNANCE AND DATA PROTECTION POLICY 2024[1]

(1) In addressing the challenges of data management, governance, and protection, the National Data Governance and Data Protection Policy 2024 was developed to promote the responsible use of data across both the public and private sectors.

(2) The policy emphasizes transparency, accountability, and the ethical use of data, while safeguarding it from unauthorized access, misuse, manipulation, or destruction.

(3) It sets clear directives for data governance, protection, privacy, and accessibility, aligning with international best practices. Key focus areas include data classification, data security, secure data sharing, and regulatory oversight to support the country's digital transformation.

(4) Public bodies are encouraged to implement secure data-sharing practices, adopt robust cybersecurity measures, and utilize digital platforms such as the e-Government Cloud to

[1] Department of Information and Communications Technology. (2024). *National Data Governance and Protection Policy*. Government of Papua New Guinea. https://www.ict.gov.pg/ndgdpp

enhance service delivery. Meanwhile, open data initiatives aim to drive economic development, support research, and promote public accountability—while ensuring sensitive data remains protected.

(5) Data standards and guidelines play a critical role in operationalizing this policy by providing consistent frameworks and technical guidance that enable secure, interoperable, and efficient data management across all sectors.

PART II. – DATA MANAGEMENT.

10. OVERVIEW

(1) This Part prescribes standards for the management of government and personal data across all national, provincial, and local-level agencies.

(2) The objectives of the following standards are to;
- (a) ensure data across all systems is collected, stored, used, and disposed of in a secure, ethical, and efficient manner that upholds the rights of individuals,
- (b) supports data-driven decision-making, and
- (c) aligns with the PNG Digital Transformation Policy 2020, Data Protection and Data Governance Policy 2024, existing and international standards.

(3) All government data must;
- (a) uphold the PNG Constitution, Public Services (Management) Act, and all data protection laws.
- (b) be stored and processed in a way that respects PNGs sovereign control over its information.
- (c) recognize the diversity of people, language, and customary systems.
- (d) be protected from misuse, loss, or unauthorized access.

(4) All public body must manage electronic data in strict compliance with Part IV of the Digital Government Act 2022.

(5) All public bodies must ensure the data is collected, stored, and processed in a responsible way in compliance with all applicable laws, regulations, standards, and guidelines.

(6) All public bodies must establish appropriate security measures, such as access controls, encryption, and firewalls, to protect the data from unauthorized access, disclosure, and misuse.

11. DATA MANAGEMENT STANDARDS

Standard 1: Data Management Life Cycle

(1) The Data Management Life Cycle provides a structured framework for managing government and personal data from its creation to its final disposal.

(2) It ensures that data is consistently collected, processed, stored, used, shared, retained, and securely destroyed.

STANDARD 1. 1 DATA CREATION

i. Data Collection

(1) Public bodies must collect and store all government data in electronic form.
(2) All public bodies must use an authorized and vetted electronic device able to collect, process, and store electronic data, ensuring electronic data collection devices and platforms are reliable, support offline/online data synchronization and is compatible with other systems. In this case, ensure compatibility with other systems by adhering to defined API standards. This enables seamless data synchronization and integration with central repositories and other government systems.
(3) In the case that electronic data collection cannot be done under (1), ensure all data that is collected manually or is converted to electronic form, if using paper-based solutions.
(4) Public bodies must standardize all forms of data collection to ensure data entry remains consistent.
(5) For the safe collection, storage, and transport of paper-based or other non-electronic data from its origin to a digitization center, ensuring data is protected from loss, damage, or unauthorized access, the table below highlights some guidelines for secure physical handling.

Guideline	Description
Controlled Access	Limit access to physical data to authorized personnel only.
Proper Storage	Store documents in locked cabinets or secure rooms with environmental controls (temperature, humidity) to prevent damage.
Transport Security	Use tamper-evident containers and trusted personnel when moving data between locations.
Handling Protocols	Minimize handling to reduce risk of loss or damage; use gloves or clean hands if necessary.
Inventory and Tracking	Maintain a log of all physical data items, recording their location, movement, and responsible staff.
Incident Preparedness	Have procedures for reporting lost, stolen, or damaged physical data.

Retention Compliance	Keep physical data only as long as required by business, legal, or regulatory requirements.

(6) When converting manual data into electronic form, the table below sets guidelines for a standard digitization process;

Stages	Details	Guidelines
1. Preparation	Collect and organize all physical data to be digitized. Remove duplicates, damaged items, or irrelevant documents.	Ensure proper labeling and inventory of documents before digitization.
2. Equipment Setup	Set up required tools such as scanners, OCR software, or manual entry forms.	Use technology suited to the data type and local context.
3. Data Scanning / Capture	Scan physical documents or manually enter data into electronic systems.	Ensure high-quality scans and accurate data entry; adjust scanner settings for clarity.
4. Quality Assurance Check	Review scanned or entered data for errors, missing fields, or misalignment.	Use double-entry verification or sampling checks for accuracy.
5. Data Validation	Compare digitized data against original records to confirm completeness and correctness.	Maintain audit logs for validation checks.
6. Metadata Assignment	Tag digitized data with relevant metadata such as owner, date, classification, and retention period.	Ensures future retrieval, tracking, and classification compliance.
7. Secure Storage	Save digitized data in secure systems with access controls and backup procedures.	Encrypt sensitive data and maintain redundancy.
8. Documentation & Traceability	Maintain records of the digitization process, including who performed it, dates, and any issues encountered.	Supports auditing, accountability, and future reference.

ii. Data Formats

(1) All data must follow pre-agreed data formats and standards (e.g. data format for dates DD-MM-YYYY, IDs may be a 10-digit numeric).

(2) Standardized data formats ensure that data is consistent, interoperable, and easily processed across systems, applications, and organizations.

(3) By adopting common formats for text, dates, numbers, identifiers, and structured files (e.g., JSON, XML, CSV), organizations reduce errors, improve data quality, and facilitate integration and sharing. Metadata standards further provide context and traceability for all data assets.

(4) The following table lists common standardized data formats and specifications.

Category	Standard	Specification
Text Encoding	Use UTF-8 for all textual data	Ensures consistency, supports international characters
Date Format	ISO 8601 (YYYY-MM-DD)	Use YYYY-MM-DDThh:mm:ss for date-time values
Number Format	Standard decimal notation	Fixed decimal places, no locale-specific formatting
Boolean Values	true/false or 1/0	Must be consistent across systems
Identifiers	Unique IDs (UUIDs or numeric IDs)	IDs must be consistent and unique across systems
Structured Data	CSV, JSON, XML	Preferred for data interchange; ensure schema consistency
Documents	PDF/A for archival, DOCX/ODT for working documents	Standardize formats for readability and long-term storage
Images	JPEG, PNG	Store metadata in EXIF or sidecar files
Data Interchange	RESTful APIs using JSON or XML	Use proper MIME types
Mandatory Metadata	Owner, creation/modification dates, source, purpose, sensitivity level	Use standardized vocabularies (Dublin Core, ISO 19115 for geospatial data)
Data Validation	Mandatory fields, numeric ranges, string patterns, referential integrity	Apply validation rules at entry and processing
Encoding of Special Characters	Escape special characters in JSON/XML	Prevent syntax errors and parsing issues
File Naming Conventions	Use descriptive, consistent, and versioned file names	Include dates, version numbers, and avoid spaces/special characters

iii. Consent and Transparency

(1) Consent and transparency standards ensure that individuals are informed and in control of their personal data. They define how consent must be collected, documented, and withdrawn, and require organizations to clearly communicate processing activities.

(2) These standards also enforce data subject rights, such as access, correction, erasure, restriction, objection, and data portability, thereby promoting accountability, trust, and compliance with national and international data protection laws.

(3) It is important data collectors get clear and informed consent from individuals before collecting their data, unless there is a legitimate reason not to do so. The table below further highlights these standards and specifications.

	Standard	**Specification**
Lawful Basis for Processing	Obtain consent or have a legal/contractual basis before processing personal data	Consent must be freely given, specific, informed, and unambiguous
Informed Consent	Provide clear and concise information to data subjects about the purpose, scope, and use of their data	Include who will process the data, how it will be used, retention period, and rights
Consent Documentation	Record and maintain proof of consent	Include date, time, method, and scope of consent
Right to Withdraw Consent	Allow data subjects to withdraw consent at any time	Withdrawal must be as easy as giving consent; update records and cease processing
Transparency of Processing	Clearly communicate data processing practices to data subjects	Publish privacy notices or statements in accessible formats
Access Rights	Data subjects have the right to access their personal data	Organizations must respond within defined timelines and provide data in a readable format
Correction / Rectification	Allow data subjects to correct inaccurate or incomplete data	Update systems promptly and notify any relevant third parties
Data Portability	Enable data subjects to receive their data in a structured, machine-readable format	Support interoperability between systems and ease of transfer
Right to Erasure (Right to be Forgotten)	Allow deletion of personal data where legally permissible	Delete securely from all storage and backups, and notify relevant parties
Restriction of Processing	Allow data subjects to request limits on how their data is processed	Apply technical and administrative controls to enforce restrictions
Objection to Processing	Data subjects can object to processing for direct marketing or profiling	Implement processes to stop processing immediately when objection is valid

Automated Decision-Making	Inform data subjects if decisions are made solely on automated processing	Provide meaningful explanations and enable human intervention when needed

(4) Inform individuals about the data being collected, the purpose of collection, and how it will be used. When getting consent, consent must be clear, specific, and freely given. Individuals should understand what personal data is collected, why it is collected, how it will be used, and who will process it. Consent should be obtained actively, for example, through opt-in checkboxes, and not pre-checked boxes. Separate consent should be requested for different purposes, such as marketing or research. Organizations must keep records of consent, including when and how it was given, and provide easy ways for individuals to withdraw their consent at any time.

(5) All Privacy notices and consent forms should be written in plain, simple language that is easy to understand. It is important to avoid technical terms, legal jargon, or long paragraphs. Use bullet points, headings, and visual aids like icons or infographics to make information easier to read. Key information should appear first, with links or expandable sections for more detail. Notices should be translated into local languages where needed and follow accessibility standards to ensure everyone, including people with disabilities, can understand them.

iv. Data Minimization

(1) Public bodies must only collect have required data for the intended purpose.

(2) Public bodies should reduce the horizon of data collection for specific and concise data that is essential in achieving a specific goal. This means that data that is not necessary to achieve the intended purpose cannot be lawfully collected, stored, or otherwise processed.

(3) The key elements of Data Minimization are:

(a) Purpose limitation: Data should only be collected for clear, defined, and lawful purposes.
(b) Relevance: The data collected must be directly relevant to the task or function being performed.
(c) Necessity: Only the data that is strictly necessary should be collected—nothing excessive or superfluous.
(d) Retention control: Data should not be kept longer than necessary. It must be securely deleted when it's no longer needed.

v. Data Validation

(1) All data should be validated during data entry to check for errors, inconsistencies, and missing values.

(2) The following table names data validation standards and specifications.

Standard	Requirement / Specification
Data Validation	Validate all data at the point of entry to detect errors, inconsistencies, and missing values.
Completeness Checks	Ensure all mandatory fields are filled; use skip logic and conditional questions to collect relevant data.
Quality Assurance	Establish procedures for validation during collection, using digital tools such as dropdown menus, automatic formatting (dates, phone numbers), and error prompts.
Ongoing Review	Conduct regular data quality reviews and cleanups to maintain accuracy and integrity.

vii. Collecting Personal Information

(1) This standard applies to data collected from individuals.

(2) Data must be processed in line with the individuals' rights. This includes:

(a) Right of Access: Individuals can request and receive a copy of their personal data.

(b) Right to Rectification: Individuals can request correction of inaccurate or incomplete data.

(c) Right to Erasure: Individuals can request deletion of their data under certain conditions.

(d) Right to Restrict Processing: Individuals can limit how their data is used.

(e) Right to Data Portability: Individuals can receive their data in a structured, machine-readable format and request transfer to another organization.

(f) Right to Object: Individuals can refuse certain uses of their data, such as direct marketing, and may object to other processing based on legitimate interests or public tasks.

STANDARD 1.2 DATA PROCESSING AND STORAGE

(1) Public bodies must store all electronic data a Single-Source of Truth (SSoT), may it be the National Electronic Data Bank or the Central Electronic Data Repository, establishing a primary data source under Section 27 and Section 28 of the Digital Government Act 2022.

(2) Public bodies must;

(a) ensure personal data is processed in a lawful, fair and transparent manner in relation to data subjects.
(b) ensure data is accurate, complete, and up to date.
(c) Implement processes for correcting inaccuracies.
(d) Maintain the integrity of data by preventing unauthorized alterations or deletions.
(e) implement role-based access controls to ensure that only authorized personnel can access or modify data.

(3) Maintain logs of data access and modifications to enable tracking and auditing.

ii. Storage Limitation

(1) Data must be kept in a form that makes it possible to identify data subjects for no longer than is necessary for the purposes of the processing.

(2) Personal data may be kept for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

(3) There should be a policy setting standard retention periods wherever possible, to comply with documentation requirements (see standards on Data Retention).

(4) Periodically review the data you hold, and erase or anonymize it when you no longer need it.

(5) Note that it is important to consider any challenges to your data retention. Individuals have a right to erasure if you no longer need the data.11

iii. Data Sovereignty Compliance

(1) All data collected, processed and stored on behalf of the Government of Papua New Guinea (PNG) must remain subject to PNG's legal jurisdiction.

(2) All service providers must demonstrate that no government data will be subject to foreign laws without explicit written content from the PNG Government.

(3) Conduct thorough risk assessments to identify potential threats to data, especially in regard to cross-border transfers.

iv. Data Localization Requirements

(1) All classified, personal and sensitive data must be stored and processed within PNG, unless a valid legal exception is made.

(2) Public cloud providers must store such data mentioned in 1.11 within a local data center, or through government-authorized cloud platform such as the Central Electronic Data Repository.

(3) For non-sensitive data or any operational data stored offshore, a local backup copy must be maintained in PNG.

(4) Public bodies must maintain control over data stored within PNG, ensuring it is not improperly accessed, transferred, or processed outside the country without compliance.

(5) In the case that a cloud or third-party service provider is used, these services must comply with PNG's data sovereignty and localization laws.

v. Data Storage Controls

(1) Government data may be stored in two ways and includes;

a) On-Premise Data Storage
b) Cloud Storage

(2) Duplicate storage of government data must be avoided unless required for backup, legal or regulatory purposes.

vi. Storage Infrastructure

(1) Government data must be hosted on infrastructure that meets minimum security certifications as those mentioned in ISO/IEC 27001 and the existing standards and guidelines (e.g. PNG Government Cybersecurity Standards, Guidelines and Best Practices 2023).

(2) Physical and logical controls must be implemented to prevent unauthorized access.

(3) Public bodies must document the physical location of all data managed.

vii. Storage Media and Environment

(1) Specifications include;

Spec	Description/Name	Specifications
1	Secure Storage Locations	• Server rooms must be locked and access restricted. • Entry logs must be maintained.
2	Environmental Conditions	• Recommended temperature: 18-24*C; Humidity 35-50% • Where air-conditioning is unavailable, use sealed-insulated storage with silica gel or moisture absorbers.
3	Power Protection	• All servers and sensitive devices must be connected to a UPSco unit. • Backup generators should be in place for critical locations where power is unreliable.
4	Fire and Water Safety	• Install smoke detectors and fire extinguishers. • Media should be stored in waterproof and fireproof cases where possible.
5	Dust and Contaminant Control	• Avoid storing data in exposed environments. • Use sealed cabinets in dusty or coastal locations.

viii. Cloud Storage Governance

(1) Cloud storage providers must:

a) Be certified under relevant security standards (e.g., ISO/IEC 27001, SOC 2).
b) Disclose the geographic location of their data centers.
c) Provide legally binding assurances that data stored in the cloud will not be transferred outside PNG without authorization.

(2) Public bodies using international cloud providers must implement data residency controls and access restrictions and ensure that contracts include data localization clauses.

ix. Data Backup and Redundancy

(1) Public bodies must perform regular backups of critical and classified data, and store at least one backup copy within PNG.

(2) Backup data must be encrypted and tested periodically for integrity and recoverability.

(3) Define and document disaster recovery.

STANDARD 1.3 DATA USAGE

(1) The following standards define the conditions under which government data can be accessed, used, shared, or reused across public sector entities and with approved external partners, including the private sector.

(2) This is important in protecting the integrity, confidentiality, and sovereignty of government data.

(3) All data usage must remain;

(a) lawful and transparent through ensuring data complies with relevant laws and policies and be communicated clearly to stakeholders.

(b) purpose-specific and be used strictly for the purpose it was collected and approved for.
(c) minimal data collection with only the minimum amount of data required for the intended purpose should be used.
(d) accountable and auditable for data usage by ensuring government data is recorded and traceable for auditing and accountability. For instance, all API calls and interactions involving data must be logged and auditable to ensure full traceability and accountability. Logs should capture relevant details such as timestamp, user or system ID, action performed, and data accessed..

(4) All data usage practices must align with relevant policies, laws and regulations.

ii. Documentation Specifications

(1) These following must be documented to ensure good data usage practices;

(a) Data Usage Agreements (DUAs) must be in place for inter-agency or third-party access and clearly define purpose, duration, and access controls. This also includes cloud service providers handling government data.

(b) Metadata Standards must be used to ensure consistency and traceability.

(c) Access Controls and Permissions must be role-based and aligned with data sensitivity.

(d) Usage Monitoring should be automated and documented for transparency and incident response.

(e) Data Deletion and Retention practices must follow DICT's retention schedules and disposal protocols.

iii. Consent and Legal Basis for Personal Data Usage

(1) Where personal data is involved:

(a) Consent must be freely given, informed, and specific.

(b) Usage without consent must have explicit legal backing, e.g. for public health, national security, or legal compliance.

(2) Individuals have the right to withdraw consent at any time, without penalty.

STANDARD 1.4 DATA SHARING

(1) These standards ensure data is shared responsibly, securely, and effectively across government, private sector, and civil society.

i. Secure Data Transfers

(1) Ensure that all data transferred across borders is done so securely, with encryption ` and secure transmission protocols in place.

(2) When transferring data internationally, ensure compliance with APEC Cross- Border Privacy Rules and other international standards for data protection.

ii. Data Sharing Agreements

(1) A Data Sharing Agreement is a formal, binding document that defines how data is shared between parties. Data sharing agreements ensure security, legality, accountability, and data integrity throughout the data exchange process. Legal and procedural frameworks to formalize data exchange between agencies and stakeholders.

(2) The data sharing agreement must clearly define why data is being shared, be aligned with legal basis and public interest and promote transparency, trust and data sovereignty.

(3) Data sharing agreements must apply to:

(a) Government-to-Government (G2G) sharing (e.g., between DICT and another ministry).

(b) Government-to-Private Sector (G2B) partnerships (e.g., telecom, banking, fintech, health providers).
(c) Government-to-Civil Society/NGOs (G2C) engagements.
(d) Cross-Border Transfers where data leaves PNG jurisdiction.

STANDARD 1.5 DATA RETENTION AND ARCHIVAL

(1) Data retention Personal Data should not be kept longer than is necessary for the purpose for which it has been collected.

(2) Data should be classified according to sensitivity, retained in a secure and organized manner, and regularly reviewed to avoid unnecessary storage. Retained data must remain protected for confidentiality, integrity, and availability, and when it is no longer needed, it should be securely disposed of.

(3) The following table shows an example of retention by data type;

Data Type	Retention Period	Archival Method
Employee Records	7 years after termination	Encrypted storage, offsite backup
Financial Records (Invoices, Receipts)	10 years	Digital archive, physical offsite storage
Customer Personal Data	5 years after last interaction	Secure encrypted storage
Emails and Communications	3 years	Email archival systems
Legal and Contractual Documents	Life of contract + 6 years	Document management system, offsite archive
System Logs / Audit Trails	2 years	Centralized log repository

(5) Data archival also ensures ensure that data no longer in active use is stored safely and can be accessed when needed.

(6) Data should be kept in widely supported formats, protected with security measures like encryption, and regularly checked for integrity. Archives should be organized for easy search and retrieval, backed up in multiple locations, and maintained so that important information remains available over time.

(7) Organizations must have defined procedures for handling old or inactive data. This includes archiving data securely for future reference when needed and disposing of data safely when it is no longer required, using methods that prevent unauthorized recovery or misuse.

STANDARD 1.6 DATA DISPOSAL AND DESTRUCTION

(1) Data must be destroyed or securely disposed of when it is no longer required.

(2) Use methods compliant with NIST SP 800-88 (e.g., cryptographic erase, shredding physical media).

(3) All data owners must maintain records of data disposal for audit purposes.

(4) Review archived data periodically; declassify or delete data no longer required under retention policies.

(5) Only authorized personnel can approve data disposal.

PART III. - DATA CLASSIFICATION

12. OVERVIEW

(1) This Part sets out standards and guidelines for data classification levels, establish criteria for classification, and the responsibilities of data custodians and stewards in applying these standards.

(2) It also establishes controls and handling requirements associated with each classification level.

(2) The main objectives of these standards are to;

(a) maintain consistent data handling across the public sector,
(b) improve risk management related to data access and misuse,
(c) enhanced interoperability and secure data sharing across agencies and systems,
(d) protect personal and/or sensitive information, in line with national data protection principles.

(2) By standardizing data classification practices, this Part ensures that all data is managed in a way that safeguards national interests, individual privacy, and institutional integrity.

13. DATA CLASSIFICATION STANDARDS AND GUIDELINES

Standard 3 Data Classification Levels

STANDARD 3.1 DATA CLASSIFATION LEVELS

(1) Data must be classified based on its sensitivity, value, criticality and legal requirements, and assign it the proper classification in compliance with Section 45 of the Digital Government Act 2022.

(2) All data must be classified into the following categories:

Classification Level	**Description**
Top-secret data	Top secret data must be given the highest protection, whose unauthorized disclosure could be anticipated to have very serious damage to national security.
Confidential data:	Confidential data must be used to protect information whose unauthorized disclosure could reasonably be anticipated to have little to serious damage to national security. This data can be further categorized into either; i. Internal Use Data ii. Restricted/Highly Sensitive Data Where internal use data must be used to protect information body only, and restricted or highly sensitive data are confidential data that must not be shared due to privacy, intellectual property or national interests.
Open Data:	Open data must be used for public data, otherwise known as information, that does not need protection and can be accessed freely. There are no restrictions on who has access to this data, but it is not modifiable.

Table 1 Classification Levels

(3) Data must be labelled clearly and accordingly to identify classification levels, and storage, access and security must reflect classification levels.

STANDARD 3.2 CLASSIFICATION CRITERIA

(1) In accordance with Papua New Guinea's Data Protection and Data Governance Policy and international best practices (ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-60), this section defines the criteria used to classify data.

(2) Data may be classified using a structure approach that ensures consistent handling, secure storage and controlled sharing of data. This includes;

(a) Identifying Data

(b) Assessing Sensitivity and Risk

(c) Assigning Classification Level

(d) Labelling and Marking

(e) Applying Security Controls

(f) Reviewing and Updating

(3) The table highlights the standardized data classification process.

Stages	Objective/Goal	Steps involved	Outcome
1. Identify Data Assets	Determine what data exists in the organization	- Conduct a data inventory across all systems, databases, applications, and physical records. - Identify data types: structured (databases, spreadsheets), unstructured (emails, documents), semi-structured (logs, XML files). - Assign data ownership: each dataset has a responsible owner accountable for classification and protection.	A complete catalog of data assets with assigned owners.
2. Assess Data Sensitivity and Value	Evaluate how sensitive or valuable each data asset is	- Determine confidentiality needs: Who should access this data? What is the risk if disclosed? - Evaluate integrity requirements: Impact if data is altered or corrupted. - Assess availability requirements: Consequence if data becomes unavailable. - Consider legal, regulatory, and	Each dataset has a preliminary sensitivity assessment indicating its potential impact if compromised.

		contractual obligations (e.g., PII, financial data, health records).	
3. Assign Classification Levels	Categorize data based on sensitivity and impact	- Apply a standardized classification scheme: • Public/Open – Minimal impact if disclosed. • Internal/Restricted – Minor risk if exposed. • Confidential/Sensitive – Requires protection, potential risk to individuals/org. • Highly Confidential/Critical – Severe consequences if compromised. - Document classification in a metadata registry, including rationale, owner, and date assigned.	Data assets are clearly labeled, enabling appropriate handling.
4. Apply Handling and Security Controls	Protect data according to its classification	- Define access controls: Who can view, edit, or share the data. - Determine encryption requirements for transmission and storage. - Specify sharing and transmission rules (e.g., confidential data cannot be sent via public email). - Set backup, retention, and disposal procedures based on classification.	Data is protected in alignment with its sensitivity level, reducing risk of breaches or misuse.
5. Monitor, Review, and Audit	Ensure classifications remain accurate over time	- Conduct periodic audits to check compliance with classification and handling rules. - Review classification during system upgrades, data migrations, or organizational changes. - Adjust classifications if data sensitivity or business context changes.	Data remains accurately classified, and protection measures remain effective.
6. Declassification and Secure Disposal	Safely reduce protection level or destroy data when no longer sensitive	- Re-evaluate necessity of protection for older data. - Declassify data if no longer poses risk. - Apply secure disposal methods: • Physical destruction (shredding, incineration).	Unnecessary sensitive data is removed, reducing storage costs and exposure risk.

		• Secure digital deletion (wiping, degaussing, overwriting).	

GUIDELINE 3.3 DATA CLASSIFICATION LEVELS AND SECURITY CONTROLS

Classification Level	Description	Examples	Security Controls
Public	Data intended for open access with no risk if disclosed.	Published laws, press releases, public datasets, Public government information/news	Integrity checks, version control, open access protocols No restriction; although verify authenticity before publication.
Confidential	Data whose disclosure may cause **moderate harm** to individuals, organizations, or government credibility.	Personal Identifiable Information (PII), medical records, financial details, commercial contracts.	Encryption at rest and in transit (AES-256, TLS). Strong authentication (MFA for remote access). Role-based access with least privilege enforcement. Audit logging & regular monitoring. Secure disposal (shredding, data wiping). Data Loss Prevention (DLP) policies. NDAs for staff

	Restricted/Highly-Sensitive - Data whose unauthorized disclosure could cause **serious harm** to government operations, public order, or critical services.	Cabinet papers, confidential government contracts, sensitive law enforcement operations.	Mandatory encryption Strict need-to-know basis, with formal approval for access. Privileged Access Management (PAM). Segmented networks (air-gapped or zero trust). 24/7 monitoring & intrusion detection/prevention. Offline and encrypted backups. Incident response procedures specifically for data breaches.
	Internal Use - Data intended for internal operations, not for public release, but whose disclosure poses **low risk**.	Internal memos, draft reports, routine operational data, HR records.	Access limited to employees/partners (role-based access control). Authentication via username & password (basic identity management). Standard backups and patch management. Logging of access for accountability.

Top-Secret	Data whose unauthorized disclosure could cause **severe harm** to national security, economy, public safety, or diplomatic relations.	National security intelligence, classified defence documents, strategic infrastructure blueprints.	Highest level of encryption. Multi-factor + biometric authentication. Strict compartmentalization and clearance vetting. Dedicated secure facilities (SCIF – Sensitive Compartmented Information Facility). Continuous monitoring, threat hunting, and zero-trust architecture. Regular penetration testing and red-teaming. Secure destruction procedures (degaussing, incineration).

STANDARD 3.4 USAGE GUIDANCE

(1) All data classifications must be respected in usage decisions, with specific handling protocols for each classification.

(2) The following table outlines specifications for data usage based on each data classification.

Classification Level	Usage Rules
Public	- Freely shareable with the public - Can be stored on public platforms - Must maintain accuracy & integrity

Confidential	- Use limited to staff with need-to-know - Share externally only under NDA/MoU/contract - Transmission via encrypted/approved channels - Not for personal email or cloud storage
	Internal Use: - Use restricted to employees/authorized partners - Share only on intranet or secure platforms - Not for external release without approval
	Restricted: - Strictly need-to-know basis - Sharing requires documented authorization - Transmission only via secure encrypted channels - Prohibited on personal/unapproved devices - Must be logged and monitored
Top Secret / National Security	- Access only by cleared personnel - Use restricted to secure facilities (SCIFs) - No sharing outside approved secure networks - Remote access generally disallowed - Copies logged, tracked, and tightly controlled

(3) Principle of Least Privilege must always be maintained where users should only have access to the data they need.

(4) When using electronic systems, ensure all access controls and logging are enforced on each classification level.

STANDARD 3.5 RETENTION AND DISPOSAL BASED ON CLASSIFICATION LEVEL

(1) Based on the classification level, the following must be applied during data retention and/or disposal.

Classification Level	Retention	Disposal
Public	Retain as long as required for business or legal purposes; can be archived indefinitely for reference.	Standard deletion or archival. No special disposal required.

Confidential	Retain only as long as necessary for business/legal requirements (e.g., HR records 7 years, financial data per tax law).	Secure deletion (data wiping) for digital records; shredding/cross-cut shredding for physical documents.
	Internal Use: Retain according to operational needs (typically 3–7 years) or as per regulatory/organizational policy.	Delete using normal IT processes; paper documents recycled or shredded.
	Restricted : Retention period defined by law, regulation, or organizational mandate (often longer-term due to sensitivity).	Secure deletion with certified tools, cryptographic wipe, or degaussing; physical destruction of paper/media.
Top Secret	Retain only for mandated period by national security law/policy; continuous review required.	Destruction by certified secure methods (incineration, degaussing, shredding to classified standards). Disposal must be logged and verified.

(2)Note that retaining data for too long increases risk exposure, particularly for personal and sensitive information, so organizations must balance business value, legal obligations, and data protection risks.

(3) For disposing of data, it is important to have good practices implemented to prevent unauthorized access, breaches, or misuse of sensitive information after its useful life.

STANDARD 3.5 DATA DE-CLASSIFYING

(1) (2) Throughout the data lifecycle, it should be periodically assessed to whether its classification level remains appropriate. This may result in the data being de-classified.

(2) Data declassification must be based on a formal assessment of risk and potential impact of disclosure of data.

(3) Only data owners are responsible for authorizing declassification of data ,and all decisions must be well-documented and auditable.

(4) Declassification must respect PNG laws, regulatory obligations, and contractual confidentiality requirements.

(5) Data may be considered for declassification if:

(a) The risk of harm from disclosure has been mitigated or no longer exists.

(b) The legal or regulatory retention period has expired.

(c) The data has been anonymized or aggregated so individual identification is no longer possible.

(d) The business, operational, or strategic sensitivity of the data has decreased.

(d) The data has been reviewed and approved by the designated data owner or custodian.

PART IV. - DATA PROTECTION.

14. OVERVIEW

(1) This Part sets out specifications that ensure that personal and sensitive data is collected, stored, processed, shared, and disposed of in a way that protects the privacy, rights, and freedoms of individuals.

(2) These specifications align with the National Data Governance and Data Protection Policy and are especially important for both public and private sector data management, and applies to all data collection, use, storage, sharing, and disposal—whether digital or physical.

15. DATA PROTECTION SPECIFICATIONS

(1) All personal data must be processed lawfully and fairly, respecting the rights and freedoms of individuals.

(2) Data should only be collected for legitimate, specific, and clearly defined purposes, and only the minimum amount necessary should be collected and retained.

(3) Accuracy must be maintained throughout the data lifecycle, and outdated or incorrect data must be corrected or deleted promptly.

(4) Data must not be retained longer than necessary and should be secured through appropriate technical and organizational measures.

(5) Public bodies must be accountable and able to demonstrate compliance with these principles.

Specification	Requirement	Minimum Controls/Specifications
Governance	Every agency must appoint a Data Protection Officer (DPO) accountable for compliance.	- DPO reports to senior management. - Maintain Data Protection Policy. - Maintain Record of Processing Activities (RoPA). - Conduct Data Protection Impact Assessments (DPIA) for new projects.
Collection	Personal data must be collected lawfully, fairly, and with informed consent (unless lawful exceptions apply).	- Consent must be informed, explicit, specific. - Use clear language in privacy notices. - Log all consent and withdrawals. - Collect minimum necessary data.
Processing	Data must be processed in line with Privacy by Design and Default.	- Limit access by least privilege. - Pseudonymise/anonymise where possible. - Enable data portability (JSON, XML, CSV). - Ensure audit logs for all processing.
Sharing & Transfer	Data Sharing Agreements (DSAs) required for all inter-agency/third-party sharing. Cross-border transfers must be controlled.	- Secure channels (VPN, SFTP, encrypted APIs). - Cross-border transfer only with DICT approval or adequacy safeguards. - Maintain register of all transfers. - Breach liability clauses in DSAs.
Storage	All sensitive data must be encrypted and access controlled.	- Databases encrypted (AES-256). - MFA required for privileged access. - Penetration testing annually. - Separate backups stored securely in PNG. - Apply ISO/IEC 27001/27040 controls.
Retention & Disposal	Data must not be retained longer than necessary. Disposal must be secure and documented.	- Define retention schedule by category (per National Archives Act). - Automate deletion where feasible. - Apply cryptographic wipe / shredding. - Maintain disposal logs and DICT oversight for classified data.

Data Subject Rights	Citizens must be able to exercise their data rights easily.	- Right to access, correction, erasure, restriction, portability. - Respond to requests within 30 days. - Provide data in machine-readable formats. - Log all requests and responses.
Incident Management	Breaches must be managed promptly with formal processes.	- Breach notification to DICT within 72 hours. - Notify affected individuals if risk is high. - Maintain breach register. - Annual review of Incident Response Plans.
Training & Awareness	Staff and citizens must be regularly trained.	- Annual mandatory training for all staff. - Specialized training for IT, HR, legal. - Public awareness campaigns on data rights. - Contractors must undergo onboarding.
Children's Data	Stronger safeguards for personal data of under-18s.	- Parental/guardian consent required. - No profiling or targeted marketing. - Apply stricter security (encryption, access logging). - Schools and health systems must follow dedicated safeguards.

PART VI. – MISCELLANEOUS.

16. IMPLEMENTATION SCHEDULE

(1) The Data Standards and Guidelines is effective from [01. 01. 2026].

(2) All public bodies must meet the requirements presented in this instrument on or before [01. 12. 2026].

17. COMPLIANCE AND MONITORING

(1) The Department of Information and Communications Technology may conduct an assessment and evaluation report of the compliance of public bodies with this instrument.

(3) Upon request by the Department of Information and Communication Technology, 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 Department of Information and Communications Technology 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

18. COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS

- Organizations must comply with all relevant laws in PNG, including the **Privacy Act 2020**, and contractual obligations for managing data, particularly when outsourcing data processing services.
- Regularly review contracts with third parties to ensure compliance with **PNG's data protection laws**, especially regarding cross-border data transfer and storage.

19. SUPPLEMENTAL STANDARDS AND GUIDELINES

(1) The Department of Information and Communications Technology may issue supplemental standards and guidelines to support this instrument as and when required.

***Papua New Guinea Government Data Standards, Specifications and Guidelines 2025*.**

ARRANGEMENT OF CLAUSES.