FMM 02.11 Retention of financial data and records

11.1 Authority and Prescribed Requirements

- Public Finances (Management) Act 1995 (PFMA) Section 5(4) requires Departmental Heads to ensure financial accounts and records are maintained in compliance with financial management standards.

- National Library and Archives Act 1993 establishes requirements for the retention, archiving, and disposal of government records, including financial documents. It requires that any 'government publication' must have two copies deposited with the National Library. It also requires a departmental head, on request by the Director-General, an annual report of the condition of libraries and archives held by the agency.

- Tax Administration Act 2017 and Income Tax Act 2025 specifies retention periods for financial records related to taxation for a period of seven years.

- Electronic Transactions Act 2021 governs the retention, use and integrity of electronic records and transactions and legislates that the electronic version of any account or record, with specific exclusions such as trust deeds, have the same legal powers as the original record (with specific conditions on the security and identify of the record).

- Auditor-General Act 1989 outlines requirements for retaining financial data for audit purposes.

- Anti-Money Laundering and Counter-Terrorism Financing Act 2015 Requires the retention of financial transaction records for due diligence and compliance monitoring.

11.2 Relevant Standards and Supporting Documentation

- General Order 23 of the Public Services (Management) Act requires that the statute of limitations on specified employment records which includes payroll information by the employee agency is for a period of not less than seven years

- IPSAS 1 (Presentation of Financial Statements) requires entities to retain

- sufficient documentation to support the preparation of financial statements.

- ISO 15489 (Records Management) can provide guidance on the creation, retention, and disposal of records in a structured and compliant manner.

11.3 Minimum Responsibilities

Departmental heads are to establish and enforce policies for the retention and secure storage of financial data and records and to ensure compliance with retention periods specified under applicable laws and standards. The departmental head, in accordance with the National Library and Archives Act shall also prepare every five years, an inventory of all public records held by the public entity and a further inventory specifying the public records which are not to be retained.

Heads of finance are to maintain accurate and up-to-date records of all financial transactions and reports and safeguard records against unauthorised access, loss, or damage.

The Director-General of the Office of Libraries and Archives is required to establish the standards for libraries and archives.

The Finance departmental head is required to index and retain financial records within the Government's approved finance system, unless delegated to a departmental head when using an alternative approved finance system.

11.4 Mandated Policy

1. **All public entities must retain financial data and records for at least seven years to ensure compliance with legal, regulatory, and operational requirements (electronic or otherwise).**

2. **All Public Entities are required to implement the *Electronic Transactions Act 2021* (ETA) which provides for the powers to store financial data and records electronically. Public Entities are not required to retain hard copy records where its retention complies with the standards under the ETA.**

3. **Some critical records and government publications must be retained indefinitely and these are identified and guidelines for their retention are issued by the Director-General of the Office of Libraries and Archives.**

4. **Departmental heads are required to index and catalogue records in an inventory.**

11.5 Non-Mandatory Guidance

11.5.1 Definition of Financial Records

Financial records include all documents that provide evidence of financial transactions, obligations, and reports, such as:

- Evidence of procurement using public funds being followed.
- Payment vouchers, receipts, and invoices.
- Bank reconciliations and statements.
- Budget documents and financial plans.
- Annual financial statements and audit reports.

11.5.2 Secure Storage of Records

- Maintain physical records in secure, climate-controlled storage facilities, however, the Electronic Transactions Act enables the storage of records and electronic and this does not require the duplicate retention of physical records. All public entities are actively encouraged to digitialise records and appropriately destroy rather than store physical records unless required to be maintained as a physical record under legislation.
- Use encrypted digital storage systems with regular backups for electronic records. Cybersecurity and disaster recovery is paramount.

11.5.3 Implement Record-Keeping Systems

- Utilise document management systems to organise and index financial records for easy retrieval. Financial transactions recorded in IFMS and most modern financial systems are organised and indexed by the system.
- Regularly update systems to reflect changes in retention policies.

11.5.4 Conduct Regular Audits

- Periodically review retained records for completeness and accuracy.
- Ensure records meet legal and operational standards for audits and reviews and periodically review them – this is to check that they are well maintained and complete and for electronic records you are checking the

integrity of the storage (particularly on drives) and if someone has accessed without authority.

11.5.5 Plan for Disposal

- Dispose of records that have exceeded their retention period in a secure and compliant manner.
- Document the disposal process and ensure no sensitive information is exposed.

11.5.6 Specific Requirements when retaining electronic records

11.5.6.1 Accessibility

- The electronic record must be accessible for future reference by all authorised parties. So records must remain in a readable format and include any metadata or information necessary for interpretation.

11.5.6.2 Integrity

- The record must be maintained in its original form, ensuring it has not been altered or tampered with.
- Any changes made to the record (e.g., updates or amendments) must be tracked and logged.

11.5.6.3 Reliability of Storage Systems

- The electronic storage system must be secure, reliable, and capable of safeguarding data from unauthorised access, loss, or damage.
- Storage solutions should include disaster recovery and backup mechanisms to ensure record continuity.
- Records must be retained for the legally prescribed duration even if electronic.

11.5.6.4 Auditability

- Electronic records must include sufficient metadata to verify their origin, authorship, and the date of creation or modification.
- Systems must support audit trails to monitor access and changes to the records.

11.5.6.5 Specific requirements for legal recognition of electronic records

- Under the ETA, electronic records are considered equivalent to paper records, provided they meet the Act's requirements for accessibility and integrity.
- If the record requires a signature, an electronic signature that complies with the ETA must be used. The electronic signature must be unique, verifiable, and linked to the individual signing the document.
- Time-stamping may be required to validate when the electronic record was created, sent, or received.
- Electronic records must be maintained in a format that is compatible with future technological advancements or converted into accessible formats during migrations.

11.5.6.6 Technical and Operational Considerations

Cybersecurity and protection of government information is important and a responsibility of the department head. Department heads need to consider the following:

- Implement encryption for finance records to prevent unauthorised access.
- Use role-based access controls to ensure only authorised officers can view or modify records.
- Maintain regular backups of electronic records in multiple secure locations.
- Test disaster recovery procedures periodically to confirm system reliability.
- Periodically review and update storage systems to ensure they remain compliant with the ETA's requirements. Retain original metadata and ensure no loss of integrity during the process.
- Document any system upgrades, migrations, or changes that affect the records. Ensure records remain intact and accessible during system migrations or upgrades.

Further Information	frcd@finance.gov.pg
Version	1.0
Date Issued	30 June 2025