FMM 03.4 Approved Accounting Systems and IT Security

4.1 Authority and Prescribed Requirements

- Public Finances (Management) Act (PFMA)
- Electronic Transactions Act of 2021
- Cybercrime Code Act of 2016

4.2 Standards and Supporting Documentation

- Nil

4.3 Minimum Responsibilities

Department of Finance

- Provide and manage access ensuring timely updates to user permissions to the IFMS in coordination with Public Entities.
- Maintain a comprehensive register of systems integrated with IFMS.
- Evaluate and test change requests for IFMS and its integrated systems to assess potential impacts.
- Offer training programs and support resources to users of IFMS to ensure users understand their roles and the necessary security protocols that should be adopted.

Finance department head

- Authorise the use of alternative accounting systems for public entities.
- Develop and enforce policies governing the use of approved accounting systems and the security of financial information across all public entities.
- Oversee compliance with established accounting and IT security policies.
- Identify and mitigate risks associated with financial information systems, ensuring the continuity and security of financial operations.

Treasury department head

- Authorise the use of budget systems for public entities.
- Develop and enforce policies governing the use of budgeting systems.
- Identify and mitigate risks associated with financial budget systems, ensuring the continuity and security of financial operations.

Departmental Heads

- Ensure robust controls are in place to restrict access to financial information exclusively to authorised personnel.
- Conduct periodic audits to verify that access rights align with current job responsibilities.
- Maintain the integrity and confidentiality of financial data by enforcing security protocols and monitoring compliance with established policies.
- Establish procedures for reporting and addressing security breaches or unauthorised access incidents promptly.

Heads of Finance/ Head of IT

- Ensure the agency has security measures to protect financial information systems from unauthorised access, cyber threats, and data breaches.
- Conduct regular security assessments and vulnerability scans to identify and address potential weaknesses in financial information systems.
- Develop and maintain incident response plans to effectively manage and mitigate the impact of security breaches.

Internal Audit Units

- Perform regular audits to ensure adherence to accounting system policies and IT security protocols.
- Report findings to relevant authorities, recommending improvements to enhance system security and compliance.

All Users

- Comply with all established policies and procedures related to the use of financial information systems and data security.
- Use system access credentials responsibly, not sharing login information and reporting any suspicious activities.
- Handle financial data with care, ensuring its confidentiality and integrity in all transactions and communications.
- Participate in ongoing training and awareness programs to stay informed about best practices in IT security and financial information management.

4.4 Mandated Policy

1. **IFMS Approved Finance System and is the authoritative database of record for public funds and the primary accounting system for public funds accounts.**

2. **All public entities, both national and sub-national, are required to use IFMS as their accounting system unless otherwise approved by Finance department head to use an alternative approved system. Such approval is granted under specific circumstances where:**

   - the adoption of IFMS is impractical or cost prohibitive. These include cases where the materiality of the public entity's financial operations does not justify the cost of implementing IFMS,
   - technological limitations or lack of connectivity hinder its effective use,
   - instances where disaster recovery, business continuity, or emergency response measures necessitate a temporary or alternative accounting solution.
   - Additionally, entities in remote or isolated areas and those operating overseas with limited access to IFMS infrastructure may be considered for an alternative system, provided robust internal controls and reporting mechanisms are in place to ensure accountability and compliance with financial management standards.

4.4.1 Preference for Electronic Documents and Electronic Transactions

3. **In line with Section 9 of the Electronic Transactions Act 2021 (ETA), records entered in the Approved Finance System and approved by workflow by authorised users and financial delegates are the official record of those transactions where they comply with the ETA.**

4. **Physical forms may be used for information purposes or where IFMS is not used as the Approve Finance System. If there is a conflict between an electronic (or digital) document and a physical document, the electronic document shall prevail where it has complied with the ETA.**

4.4.2 IFMS System Interfaces/Integrations and Change Requests

5. **The Finance department head and Treasury department head (for Budget modules) are the system owners and authorising administrator for the IFMS and approval is required for any interfaces direct or indirect to the financial records of this system.**

6. **The Department of Finance is required to maintain an IT integration register and diagram of all systems integrated with IFMS and ensure that the impact of any IFMS change requests approved to production test for**

any impact on those integrated systems prior to their implementation in production.

4.4.3 Protection and Security of Government Financial Information and Records

7. **Persons, regardless of their employment status, fall under authority of the Cybercrime Code Act, and are subject to criminal action for offences including the unauthorised access or distribution of Government financial information or records, including, but not limited to:**

   - Intentionally remains logged onto or remains logged on or continues to use an electronic system without authorisation or after authorisation has expired (Section 11, Cyber Crime Act 2016)
   - Performing electronic forgery (Section 12, Cyber Crime Act 2016)

8. **Access to IFMS is limited to those public officers based upon their roles as determined by job requirements. Access to IFMS and the different modules are based upon a person's role, or job, in the public entity and restricts that person to the responsibilities and functions of that position, or job description.**

9. **The department head should ensure processes are in place to create, amend, and deactivate IFMS users as part of their internal human resource processing before forwarding User Access Requests to the IFMS team to assign a userid and password.**

4.5 Non mandatory Guidance

Amendments, cancellation and adding of users for IFMS form can be obtained by emailing the IFMS Service Desk service_desk@finance.gov.pg

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