REPUBLIC OF KENYA

THE NATIONAL TREASURY AND ECONOMIC PLANNING

INFORMATION SECURITY POLICY FOR PUBLIC FINANCIAL MANAGEMENT ICT SYSTEM

NOVEMBER 2023

TABLE OF CONTENTS

TERMS AND DEFINITIONS ..... **VI**

ABBREVIATIONS ..... **IX**

FOREWORD ..... **X**

VISION ..... **XI**

MISSION ..... **XI**

1.0 INTRODUCTION AND BACKGROUND **1**

1.1 SITUATIONAL ANALYSIS OF INFORMATION SECURITY RISKS 2
1.2 RATIONALE OF THE POLICY 3
1.3 PURPOSE OF THE POLICY 4
1.4 OBJECTIVES OF THE POLICY 4
1.5 OVERALL SCOPE 5
1.6 NORMATIVE REFERENCES 5
1.7 APPLICATION OF THE POLICY 6
1.8 POLICY STATEMENT 6
1.8.2 GENERAL POLICY GUIDELINES *6*
1.9 ENFORCEMENT 6
1.9.1 CHALLENGES OF INFORMATION SECURITY *7*

2.0 POLICY THEMATIC AREAS **9**

3.0 INFORMATION SECURITY GOVERNANCE **10**

3.1 MCDAs GOVERNANCE STRUCTURE 10
3.2 POLICY STATEMENT 10
3.3 GUIDELINES 10

4.0 CYBER SECURITY MANAGEMENT **12**

4.1 TELEWORKING 12
4.1.1 SCOPE 12
4.1.2 POLICY STATEMENT 12
4.1.3 GUIDELINES 12
4.2 MOBILE DEVICE MANAGEMENT 13
4.2.1 SCOPE *13*
4.2.2 GUIDELINES *13*
4.3 MALWARE MANAGEMENT 14
4.3.1 SCOPE *14*
4.3.2 POLICY STATEMENT *14*
4.3.3 GUIDELINES *15*
4.4 BRING YOUR OWN DEVICE (BYOD) 15
4.4.1 SCOPE *15*
4.4.2 POLICY STATEMENT *15*
4.4.3 GUIDELINES *16*

5.0 SYSTEMS AND APPLICATIONS SECURITY **17**

5.1 SYSTEMS ACQUISITION MAINTENANCE AND DECOMMISSIONING 17
5.1.1 SCOPE *17*
5.1.2 POLICY STATEMENT *17*
5.1.3 GUIDELINES *17*
5.1.4 MAINTENANCE OF PFM INFORMATION SYSTEMS *18*
5.1.5 DECOMMISSIONING OF PFM INFORMATION SYSTEMS *18*
5.2 APPLICATION PROGRAMMING INTERFACES (APIs) AND INTEROPERABILITY 19
5.2.1 SCOPE *20*
5.2.2 POLICY STATEMENT *20*
5.2.3 GUIDELINES *20*
5.3 VIRTUALIZATION 20
5.3.1 SCOPE *21*
5.3.2 POLICY STATEMENT *21*
5.3.3 GUIDELINES *21*

6. 0 COMMUNICATION SECURITY 22

6.1 NETWORK SECURITY 22
6.1.1 SCOPE *22*
6.1.2 POLICY STATEMENT *22*
6.1.3 GUIDELINES *22*
6.2 WIRELESS SECURITY 24
6.2.1 SCOPE *24*
6.2.2 POLICY STATEMENT *24*
6.2.3 GUIDELINES *24*
6.3 ELECTRONIC MESSAGING 25
6.3.1 SCOPE *25*
6.3.2 POLICY STATEMENT *25*
6.3.3 GUIDELINES *25*
6.4 INFORMATION SHARING 26
6.4.1 SCOPE *26*
6.4.2 POLICY STATEMENT *26*
6.4.3 GUIDELINES *27*
6.5 AGREEMENTS ON INFORMATION TRANSFER 27
6.5.1 SCOPE *27*
6.5.2 POLICY STATEMENT *27*
6.5.3 GUIDELINES *27*

7.0 INFORMATION SECURITY RISK MANAGEMENT 29

7.1.1 SCOPE *29*
7.1.2 POLICY STATEMENT *29*
7.1.3 GUIDELINES *29*
7.2 INFORMATION ASSET MANAGEMENT 29
7.2.1 SCOPE *30*
7.2.2 POLICY STATEMENT *30*
7.2.3 GUIDELINES *30*
7.3 INFORMATION CLASSIFICATION AND SHARING 31
7.3.1 SCOPE *32*
7.3.2 POLICY STATEMENT *32*
7.3.3 GUIDELINES *32*
7.4 ACCEPTABLE USE POLICY 32
7.4.1 SCOPE *33*

7.4.2 POLICY STATEMENT *33*
7.4.3 GUIDELINES *33*
7.5 BUSINESS CONTINUITY MANAGEMENT 34
7.5.1 SCOPE *35*
7.5.2 POLICY STATEMENT *35*
7.5.3 GUIDELINES *35*
7.5.3.1 BUSINESS CONTINUITY PLANNING (BCP) 35
7.5.3.2 DISASTER RECOVERY PLANNING (DRP) 36
7.5.3.3 BACKUP AND RESTORATION PLAN 36
7.6 THREAT AND VULNERABILITY MANAGEMENT 37
7.6.1 SCOPE *38*
7.6.2 POLICY STATEMENT *38*
7.6.3 GUIDELINES *38*

8.0 HUMAN RESOURCES SECURITY 40

8.1 INTRODUCTION 40
8.1.1 SCOPE *40*
8.1.2 POLICY STATEMENT *40*
8.1.3 GUIDELINES *41*
8.2 BACKGROUND SCREENING 41
8.2.1 POLICY STATEMENT *41*
8.2.2 GUIDELINES *41*
8.3 IN-SERVICE 42
8.3.1 POLICY STATEMENT *42*
8.3.2 GUIDELINES *42*
8.4 TERMINATION OR CHANGE OF RESPONSIBILITIES 42
8.4.1 POLICY STATEMENT *42*
8.4.2 GUIDELINES *42*
8.5 INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING 42
8.5.1 POLICY STATEMENT *42*
8.5.2 GUIDELINES *43*

9.0 OPERATIONAL SECURITY 44

9.1 ACCESS CONTROL 44
9.1.1 POLICY STATEMENT *44*
9.1.2 GUIDELINES *44*
9.2 CLOUD SECURITY 45
9.2.1 SCOPE *45*
9.2.2 POLICY STATEMENT *45*
9.2.3 GUIDELINES *45*
9.3 CHANGE MANAGEMENT 46
9.4.1 SCOPE *46*
9.4.2 POLICY STATEMENT *46*
9.4.3 GUIDELINES *46*
9.5 USER ACCOUNT MANAGEMENT 47
9.5.1 SCOPE *47*
9.5.2 POLICY STATEMENT *47*
9.5.3 GUIDELINES 47
9.6 PASSWORD POLICY 48
9.6.1 SCOPE *48*
9.6.2 POLICY STATEMENT *48*

9.6.2 GUIDELINES *49*

10.0 PHYSICAL AND ENVIRONMENTAL SECURITY **50**

10.1 SCOPE 50
10.2 POLICY STATEMENT 50
10.3 GUIDELINES 50

11.0 INCIDENT MANAGEMENT POLICY **51**

11.1 SCOPE 51
11.2 POLICY STATEMENT 51
11.3 GUIDELINES 51

ANNEXES **52**

ANNEX A: ICT SECURITY ROLES 52

RESPONSIBILITIES **57**

TERMS AND DEFINITIONS

A duress alarm	Is a method for secretly indicating that an action is taking place 'under Duress'.
Application Security	Application security is the use of software, hardware, and procedural methods to protect applications from external threats from development, Deployment to maintenance.
Asset	Anything that has value to the MCDA
Attack	Attempt to obtain, alter, destroy, remove or reveal information without authorized access or permission.
Availability	The property of being accessible and usable upon demand by an authorized entity
Confidentiality	The restriction of information to those persons who are authorized to receive or access it
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Data Security	Data security refers to protective measures that are applied to prevent unauthorized access to computers, databases and websites that may cause data corruption.
Email Security	Email security refers to the collective measures used to secure the access and content of an email account or service.
External Stakeholders	Entities who are outside the organization
Hardware Security	Hardware security refers to the collective measures deployed to secure the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the system.
Information	Data that has a meaning or can be interpreted. It can be held as an electronic record or in a non-electronic format such as paper, microfiche, photograph
Information Asset	Information that has value to the Institution. Key Information Assets are the most important types of information required for achievement of the Institutions' strategic objectives
Information Security	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

Information Security Management System (ISMS)	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, Maintain and improve information security.
Information security event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
Information Security incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Information Security Unit	Department/ Unit responsible for the function for information security within the institution.
Integrity	The completeness and preservation of information in its original and intended form unless amended or deleted by authorized people or processes.
Internal Stakeholders	Entities who are inside the organization
MCDA	Ministries, Counties, Departments and Agencies
MIS	Management Information System
Network Security	Network security refers to any activities designed to protect the usability, Reliability, integrity, and safety of your network and data.
Physical Security	The protection of building sites and equipment (and all information and software contained therein) from theft vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee).
Quality	The state of completeness, validity, consistency, timeliness and accuracy that makes data appropriate for both operational and strategic use.
Residual risk	The risk associated with an action or event remaining after natural or inherent risks have been reduced by risk controls
Risk acceptance	Decision to accept a risk
Risk analysis	Systematic use of information to identify sources and to estimate the risk
Risk assessment	Overall process of risk analysis and risk evaluation

Risk evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk management	Coordinated activities to direct and control an MCDAs with regard to risk
Risk treatment	Process of selection and implementation of measures to modify risk
Risk:	Any reasonably identifiable circumstance in relation to the use of network and/or information systems, - including a malfunction, capacity overrun, failure, disruption, misuse, loss or other type of malicious or non- malicious event - which, if materialized, may compromise the normal operation and security of the network and information systems.
Teleworking	Refers to all forms of work outside of the office, including nontraditional work environments, such as those referred to as "telecommuting", "flexible workplace" and remote work" and "virtual work" environments.
Threat	Any circumstance or event with the potential to adversely impact organizational operations.
Vulnerability	weakness that can be exploited by criminals to gain unauthorized access into a system

ABBREVIATIONS

API	Application Programming Interface
API	Application Program Interface
DKIM	Domain Keys Identified Mail
DMARC	Domain based Message Authentication Reporting and Conformance
GEA	Government Enterprise Architecture
GESDeK	Governance for Enabling Service Delivery in Kenya
GPS	Global Positioning System
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
InfoSec	Information Security
IS	Information Security
ISMS	Information Security Management System
ISO	International Standards Organization
IT	Information Technology
MCDA	Ministry, Counties, Departments and Agencies
NDA	Non-Disclosure Agreement
PCI-DSS	Payment Card Industry – Data Security Standard
PEFA	Public Expenditure and Financial Accountability
PFM	Public Financial Management
PFMA	Public Finance Management Act
PFMR	Public Financial Management Reform
PFMRS	Public Finance Management Reform Strategy
PIM	Public Investment Management
PIMIS	Public Investment Management Information System
PKI	Public Key Infrastructure
PPADA	Public Procurement and Asset Disposal Act
PPD	Public Procurement Department
SC	Steering Committee
VLAN's	Virtual Local Area Networks
VPN	Virtual Private Network

FOREWORD

In the Information Age, there has been massive use of technology in every facet of human life from how individuals, institutions, societies and nations interact. Though the interactions have been beneficial, there have been challenges especially in security and privacy. Systems and networks have been a target of a variety of attacks whether intentional or accidental, leading to exploitation of data for malicious purposes through computer-based fraud, data theft, surveillance or vandalism etc. The Public Financial Management (PFM) ICT systems are prone to such vulnerabilities, which could impede the progress made in the use of technology in effective, efficient service delivery and most importantly the achievement of Government development goals under Vision 2030. As a result, there is a necessitated need to develop a policy that protects against possible consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of information in PFM ICT Systems.

This policy therefore provides the framework for development and maintenance of PFM ICT systems that are flexible and efficient; secure and reliable and provides confidence in digital capabilities. Additionally, recent legislations require entities to protect data privacy and to ensure the confidentiality and security of information and its use is within the legal requirements. This policy provides the internal and external stakeholders direction and support for information security and lists a set of component sub-policy documents which taken together constitute the Information Security Policy (ISP) for PFM ICT system owners, users and authorized third parties. It is my belief that full implementation and periodic reviewing of this policy will require involvement and support, integrated vision and a set of sustained & coordinated strategies of all stakeholders. I thank all stakeholders for their participation in the development of this policy.

We hope that the team spirit exhibited during the formulation of the policy document, will be carried through to the implementation phase.

DR. CHRIS KIPTOO, CBS
PRINCIPAL SECRETARY/THE NATIONAL TREASURY

VISION

To have an ongoing and mature information security practice that is continually reducing PFM Information systems security risk exposure and data loss.

MISSION

To secure information and information assets of PFM systems, build capabilities to prevent and respond to information security threats, reduce vulnerabilities, protect the confidentiality, uphold the integrity and maintain the availability of information and information assets of PFM Systems so as to minimize damage and reduce risk across the organization.

1.0 INTRODUCTION AND BACKGROUND

The Economic Recovery Strategy for wealth and Employment Creation (ERS-WEC 2003-2007) emphasized the need for reforms in the Public Financial Management. These reforms were intended to lead to fiscal sustainability and balance in the economy, restructuring and re-allocations for growth and poverty alleviation and improved public sector performance in terms of efficiency and effectiveness in service delivery.

Consequently, the Public Financial Management Reform (PFMR) Secretariat was established in 2006 by the then Ministry of Finance to Coordinate PFM reforms within the Government. The implementation of these reforms started with the first strategy, "The revitalization of PFM systems in Kenya (2006-2011)". The promulgation of the new Constitution 2010 and thereafter the enactment of the Public Financial Management Act (2012) gave impetus for further PFM reforms.

Additionally, the need to comply with international standards as highlighted by various Public Expenditure and Financial Accountability (PEFA) assessments led to the need for sustainability of the reforms beyond the scope of the initial strategy and hence the development of the second strategy (2013-2018) and the current strategy (2018-2023).

The overall objective of the reforms is to ensure a public financial management system that promotes transparency, accountability, equity, fiscal discipline and efficiency in the management and use of public resources for improved service delivery and economic development.

The Objective is achieved through supporting reforms and capacity building in Ministries, Department and Agencies (MDAs) that are central to Public Financial Management at both the National and County Levels of Government. Currently there are thirty-three (33) MDAs that are heavily involved in the implementation of the reforms.

Automation of core PFM ICT systems and processes is a common theme that cuts across the eight result areas of the Public Financial Management Reforms Strategy 2018-2023. The Strategy has identified more than 29 PFM ICT systems that need to be developed, upgraded or maintained to ensure that they are fit for purpose in achieving Modernized PFM Information Systems. Some of the PFM ICT Systems that are in place or under development include; IFMIS reporting and budgeting, cash planning and exchequer systems, e-Government Procurement (e-GP) and State Portal, Government Human Resource Information System (GHRIS) and data warehouse, Government Investment Management Information System (GIMIS), e- Citizen Portal, Budget Portal, and Public

Investment Management Information System (PIMIS). Additional PFM Areas lined up for development of ICT Systems include Pensions Management, Public Asset and Liabilities Management, Public Performance Management,
County Fiscal Data Analysis, Integrated Devolution Data Portal, TSC
Human Resource Management Information System (HRMIS), and Integrated State Corporations Management System.

This document presents an Information Security Policy for PFM ICT Systems. The policy therefore provides the guidelines for development, acquisition, implementation, integration, maintenance and decommissioning of PFM ICT systems that are flexible and efficient; secure and reliable and provides confidence in digital capabilities. The policy also states the high-level institutional goals around expected information security behaviors and outcomes. The documents to be used to supplement this information security policy are ICT Authority Standards; Procedures; and Guidelines. The National Treasury shall ensure Compliance to this Policy.

1.1 SITUATIONAL ANALYSIS OF INFORMATION SECURITY RISKS

In information security, a SWOT analysis is useful for developing a better understanding of the security environment. It will also support the organization's overarching strategy by giving insight into security assets, risks, issues, and challenges that the PFM Information Systems face.

SWOT analysis with an information security focus has the following results;

Strengths	**Weakness**
S1. The most valuable assets have new hardware and software information security S2. Certified means of information protection S3. Multi-factor authentication is available S4. Strong data encryption practices S5. Data protection Commission	W1. Insufficient information protection system for employees who work remotely W2. Lack of regular backup system W3. Difficulties in embracing the emerging technologies W4. Lack of a written security plan/policy in MCDAs W5. Spotty update process for security patches W6. Inadequate funding for information security initiatives W7. Bureaucratic procedures in government to conform to a changing ICT driven world
Opportunities	**Threats**
O1. Establishing interaction with MCDAs O2. Outsourcing O3. Options for cloud storage for data, keeping information secure and backed up off-site O4. Advanced information technologies O5. Increased attendant automation	T1. Natural disasters T2. Staff turnover thus losing best IS staff T3. Fraudulent intrusion (hackers, computer criminals, fired employees) on the rise T4. Rapid changes in technology

1.2 RATIONALE OF THE POLICY

This policy intends to address the current PFM Information Systems challenges, such as unauthorized system access, risk to system security incidents, system data manipulation, and lack of a framework to govern system information security.

1.3 PURPOSE OF THE POLICY

The purpose of the Information Security Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to MCDAs, business partners, and our stakeholders in matters of systems development, implementation and maintenance. In particular, it is to;

1.3.1 Maintain the reputation of the organization, and uphold ethical and legal responsibilities;

1.3.2 Establish a general/ overall approach to information security;

1.3.3 Detect and foretell/predict /preempt the compromise/breaches of information security such as misuse of data, networks, computer systems and applications;

1.3.4 Observe the rights of users; and

1.3.5 Provide effective mechanisms for responding to complaints and queries concerning real or perceived non-compliances with the policy.

1.4 OBJECTIVES OF THE POLICY

Information Security is defined as the safeguarding of five primary objectives;

1.4.1 Confidentiality

- **Data confidentiality –** To assure that confidential information is not disclosed to unauthorized individuals
- **Privacy -** To assure that individual control or influence what information may be collected and stored

1.4.2 Integrity

- **Data integrity -** To assure that information and programs are changed only in a specified and authorized manner
- **System integrity:** To assure that a system performs its operations in unimpaired manner

1.4.3 Availability - To assure that systems works promptly and service is not denied to authorized users

1.4.4 Authenticity - To ensure the property of being genuine and being able to be verified and trusted; confident in the validity of a transmission, or a message, or its originator/receiver (curb against non-repudiation).

1.4.5 Accountability - generates the requirement for actions of an entity to be traced uniquely to that individual to support nonrepudiation, deference, and fault isolation among others.

The specific objectives of this policy are to;

i. Protect the PFM Information systems information assets through safeguarding its confidentiality, integrity and availability;

ii. Establish effective information security governance structure including accountability and responsibility for PFM Information systems;

iii. Maintain an appropriate stakeholder awareness, knowledge and skill to minimize the occurrence and severity of information security incidents;

iv. Ensure MCDAs are able to continue and/or rapidly recover its business operations in the event of a detrimental information security incident within PFM operational environment;

v. Ensure compliance to the relevant legal and regulatory frameworks governing PFM Information Systems; and

vi. Provide the principles by which a safe and secure information systems working environment can be established for authorized users.

vii. Implement adequate information security controls to ensure that the use of ICT resources is effective, efficient, and consistent in line the GoK information security Standards, policies, guidelines, and procedures.

1.5 OVERALL SCOPE

This Information Security Policy will address all data, programs, systems, facilities, other technical infrastructure, users of technology and third parties in a given MCDAs, without exception.

1.6 NORMATIVE REFERENCES

This Policy is not the only document that MCDAs should look to when implementing the information security stance. The policy states the high level institutional goals around expected information security behaviors and outcomes.

Other documents will be used to state the threshold of acceptable behavior, systematic processes to follow, or recommended (but not required) actions to take. The documents to be used to supplement this information security policy are but not limited to;

Constitution of Kenya 2010 Public Finance Management Act 2012 Public Procurement and Asset Disposal Act 2015 Comprehensive Logical Framework for PFM ICT Systems 2021 Government ICT Standards: Information Security Standard 2019 Public Financial Management Reforms Strategy 2018-2023

National ICT Policy 2019 Computer Misuse and Cyber Crimes Act 2018 Data Protection Act 2019

1.7 APPLICATION OF THE POLICY

This policy applies to Government institutions implementing PFM Information systems, and external stakeholders working within PFM ICT Systems operational environment. The information security framework (comprising this policy, supporting policies, processes and tools and the requisite management and decision-making structures) shall be an enabling mechanism for information sharing and for reducing information related risk to acceptable standards.

1.8 POLICY STATEMENT

MCDAs shall ensure preservation of confidentiality, integrity and availability of all its key information assets within PFM operational environment in order to maintain effective & efficient service delivery, legal and contractual compliance as well as reputation. The policy's goal is to protect PFM Information Systems operational environment against all internal, external, deliberate or accidental threats.

1.8.2 GENERAL POLICY GUIDELINES

The National Treasury and all MCDAs managing PFM ICT Systems shall;

1.8.2.1 Ensure that Information security governance is integrated into the overall enterprise governance structure hence supporting organizational goals by the information security program;

1.8.2.2 Deploy internal metrics and ensure continuous monitoring of changing security conditions;

1.8.2.3 Conduct security audits in accordance with Government regulations as well as best practice; and

1.8.2.4 Assign responsibilities related to information security and risk management.

1.9 ENFORCEMENT

The Accounting Officer in respective MCDAs shall ensure enforcement and compliance to this policy. Overall oversight rests with the National Treasury. Personnel found to have violated this policy may be subject to disciplinary action in line with the Public Service Commission Discipline Manual 2022, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions in line with the Public Procurement and Disposal Act 2015, up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

There shall be no exceptions to this policy.

1.9.1 CHALLENGES OF INFORMATION SECURITY

1.9.1.1 Lack of knowledge on online safety – the practice of maximizing the user's personal safety against security risks to private information and property associated with using the internet is not widely adopted.

1.9.1.2 Unauthorized access which may result in breach of confidentiality, alteration or loss of information.

1.9.1.3 Governance and Compliance: Information security governance is a fairly new docket in the government seeing as there are also no titles for information security personnel;

1.9.1.4 Malware;

1.9.1.5 Social engineering which involves the psychological manipulation of people into divulging confidential information. Social engineering includes phishing, pharming, fraudulent messages or calls among others.

1.9.1.6 Cloud computing presents a number of challenges for users and businesses such as:

- Reliability,
- Compromised credentials and account hijacking,
- Jurisdiction,
- Lack of privacy,
- Unsecure interfaces,
- Distributed Denial of Service,
- Increased risk through shared technology,
- Cloud service abuses,
- Limitations in investigations,
- Governance and Compliance.

1.9.1.7 Systems unavailability: This is when normal system functions are rendered unusable for reasons not limited to natural disasters, hardware failure, data

corruption, data loss, malware, denial of service (DOS). Users are prevented from accessing a critical service.

1.9.1.8 System Fraud: This is deliberate manipulation or modification of data and/or records for financial or personal gain.

1.9.1.9 Identity Theft: This is where someone uses another person's identity information such as a name, identity number, passport number, PIN, social media account, among others without permission.

1.9.1.10 The spread of untrue or misleading information over electronic media especially social media is on the increase.

1.9.1.11 Lack of security awareness by users is a major challenge in safeguarding information security.

1.9.1.12 Handheld and Mobile Devices: The increased penetration of mobile phones presents various challenges including loss of handheld and mobile devices, loss of Personal Identifiable Information (PII), data loss and exposure of confidential information. Additionally, spread of malicious applications through handheld and mobile devices is on the increase.

1.9.1.13 The level of cyber incident reporting in the country is very low and vague.

1.9.1.14 Procedures used are often counter-intuitive.

1.9.1.15 Requires constant monitoring.

1.9.1.16 Security is too often an after-thought in the onset of system design, development and roll-out.

2.0 POLICY THEMATIC AREAS

The following are the Information Security Thematic areas covered in this policy;

- **a.** Information Security Governance
- **b.** Cybersecurity Management
- **c.** Systems and Applications Security
- **d.** Communication Security
- **e.** Information Security Risk Management
- **f.** Human Resources Security
- **g.** Operational Security
- **h.** Physical and Environmental Security
- **i.** Incident Response Management

3.0 INFORMATION SECURITY GOVERNANCE

The Information Security Governance policy defines guidelines for internal organization and external entities of the information security function in order to plan, strategize, resource, and oversee the implementation and maintenance of information security within the respective scope of responsibility. The purpose of this policy is to provide an information security management framework within PFM Information systems operational environments. This will enable establishment and provision of leadership for the information security function as well as ensure efficient and effective implementation of this policy across MCDAs.

3.1 MCDAs GOVERNANCE STRUCTURE

This policy covers internal organization of information security in MCDAs managing PFM ICT systems including but not limited to management commitment to information security, co-ordination, allocation of security responsibilities, authorization process for information processing facilities, confidential agreements, third party security and contact with authorities.

3.2 POLICY STATEMENT

MCDAs shall establish structures to implement information security to manage PFM ICT systems. The accounting officer shall appoint an information security steering committee ***(see Annex B for membership)*** which shall ensure implementation of the information security policy, assign security roles and co-ordinate and review the implementation of security within MCDAs managing PFM ICT Systems.

The contacts with external security specialists or groups, including relevant authorities, shall be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents.

3.3 GUIDELINES

3.3.1 The Accounting Officer in the MCDA shall actively support information security within the MCDAs through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities;

3.3.2 MCDAs shall implement this information security policy and provide the resources needed for its implementation;

3.3.3 MCDAs shall identify the needs for internal or external specialist information security advice, and review and coordinate results of the advice.;

3.3.4 The information security co-ordination shall involve the co-operation and collaboration of officers within government institutions implementing PFM Information Systems.

3.3.5 MCDAs should clearly define and allocate information security responsibilities in accordance to this information security policy;

3.3.6 Officers with allocated security responsibilities may delegate tasks to others;

3.3.7 The National Treasury shall be responsible for reviewing this policy at planned intervals, or when significant changes to the security implementation occur.

4.0 CYBER SECURITY MANAGEMENT

Cyber security management is described as the process, which MCDAs undertake to protect information systems and computer networks from cyber-attacks and threats. Cybersecurity management covers Teleworking,
Mobile Device management, Malware management and BYOD management.

4.1 TELEWORKING

It involves working remotely away from the physical office location using technology and telecommunications to remain in touch with the business and its related systems. The purpose of this is to provide guidelines and procedures that allow PFM Information System users to work remotely in an authorized and secure manner while ensuring administrative efficiencies and supporting continuity of operation plans.

4.1.1 SCOPE

The stipulated guidelines shall cover both internal and external users of PFM information systems.

4.1.2 POLICY STATEMENT

This gives the principle guidelines of accessing the organizational resources remotely including conducting business processes.

4.1.3 GUIDELINES

4.1.3.1 MCDAs shall be responsible for clearly communicating expectations of work assignments, check-ins, and any other parameters for supporting a remote arrangement;

4.1.3.2 System users shall be responsible for ensuring that they operate in an environment that is secure and conducive for teleworking;

4.1.3.3 MCDAs shall ensure that users are sensitized and educated on the possibilities of risks associated with teleworking;

4.1.3.4 MCDAs shall identify, authenticate and authorize teleworkers before giving them access to PFM information systems resources;

4.1.3.5 Where sensitive or confidential information is being stored or accessed from off-premise, an approved access solution, such as via VPN, should be used;

4.1.3.6 Any loss or theft of equipment or personal equipment, which has been used to access sensitive PFM information while teleworking, shall be reported to the relevant authorities;

4.1.3.7 MCDAs should deploy secured equipment and/or software to ensure security is upheld in a teleworking environment.

4.2 MOBILE DEVICE MANAGEMENT

This is the process of managing and securing mobile devices deployed across multiple mobile service providers and across multiple mobile operating systems being used within the MCDAs. The Purpose of this policy is to provide PFM Information Systems users with guidelines and requirements regarding the security of data, information, and communications while using mobile devices, which include and not limited to Laptops, Tablets, and Mobile phones/Smart Phones.

4.2.1 SCOPE

This applies to all mobile devices used in creation, processing, accessing, storing and disseminating data and information in PFM Information Systems.

4.2.2 GUIDELINES

4.2.2.1 The data stored in mobile devices shall be backed up frequently and measures provided for recovery;

4.2.2.2 Usage of a mobile device to capture unauthorized images, screenshots, video, or audio, whether native to the device or through third-party applications, is prohibited;

4.2.2.3 Mobile devices accessing PFM Information Systems shall have the Device management applications, software GPS capabilities enabled to allow location transparency and information security;

4.2.2.4 All Mobile devices vulnerable to theft, loss or unauthorized access must have appropriate password, passcode or pin, cases of theft or loss of mobile devices shall be reported to the relevant authorities;

4.2.2.6 MCDAs shall plan for training of officers in using mobile devices to raise awareness of the additional risks resulting from this way of working and the controls that should be implemented;

4.2.2.7 Mobile computing devices should have time-out protection applied, which automatically lock the device after a defined period of inactivity;

4.2.2.8 Mobile devices should have up-to-date genuine firmware, operating systems, anti-malware software and applications installed;

4.2.2.9 Officers shall not permit unauthorized users including family or friends, to use or modify any mobile device provided by the MCDA;

4.2.2.10 Officers who opt to use mobile computing devices not owned by the MCDA to store or access PFM Information System are fully responsible for ensuring that the device features have adequate security provisions in order to protect the information;

4.3 MALWARE MANAGEMENT

Attacks on IT Resources by malicious software has increased with advancement in technology. This has caused organizations time and money in trying to solve the damages on the IT Resources and thereby reducing efficiency, productivity and service delivery. The PFM ICT Systems are not an exception, thus the need to have proper mechanisms in place to mitigate these vulnerabilities. The purpose of this policy is to provide measures to mitigate service disruption and restoration caused by malware attacks and provide guidelines to sensitize users on malware management.

4.3.1 SCOPE

This covers the full cycle of malware management including but not limited to identification, quarantine, remediation, scanning, and service restoration and user education.

4.3.2 POLICY STATEMENT

To achieve business objectives and continuity of operations, PFM ICT Systems owners shall adopt and follow the following guidelines to ensure the protection of IT assets from malware attacks.

4.3.3 GUIDELINES

The MCDAs shall;

4.3.3.1 Install devices accessing PFM ICT Systems with licensed antimalware solutions such as antivirus, firewalls, intrusion, detection and prevention systems;

4.3.3.2 Ensure that the anti-malware software are regularly updated;

4.3.3.3 Restrict user access to unauthorized sources such as insecure websites and programs through firewalls and related tools;

4.3.3.4 Prevent users from uninstalling or disabling antimalware agents or applications in computing devices by limiting user rights;

4.3.3.5 Isolate suspected or infected computing devices until the threat is eliminated;

4.3.3.6 Ensure devices running PFM Information systems are configured to automatically conduct anti-malware scan of removable media when inserted or connected;

4.3.3.7 Ensure devices running PFM Information systems are configured not to auto-run content from removable media or online sites;

4.3.3.8 Do regular backups of information and information assets of PFM Information systems; and

4.3.3.9 Regularly conduct user awareness on best security practices while using PFM Information systems.

4.4 BRING YOUR OWN DEVICE (BYOD)

BYOD is the practice of allowing the employees of an organization to use their own computers, smartphones or other devices for work purposes. The increasing prevalence of BYOD is set to have a fundamental impact on the management of information security. The purpose of this policy is to guide on secure usage of personal devices to access PFM ICT systems and resources.

4.4.1 SCOPE

This covers the use of devices including but not limited to mobile phones, smart phones, tablets, laptops and portable disk drive to access PFM Information Systems and resources.

4.4.2 POLICY STATEMENT

This gives the principle guidelines of allowing employees of the MCDAS to use their own computers, smartphones and other devices for work purposes.

4.4.3 GUIDELINES

Use of personal devices to access PFM Information systems and resources shall be subject to the following guidelines.

MCDAs shall;

4.4.3.1 Log and monitor all personal devices accessing their PFM Information Systems;

4.4.3.2 Regularly sensitize their users on best practices while using their own devices;

4.4.3.3 Enforce signing of an acceptance use agreement to all PFM Information system users; the acceptance use agreement shall require the user to:

a. Have up-to-date genuine firmware, operating systems, anti-malware software and applications installed.

b. Use authorized applications only to access PFM Information systems

c. Ensure access to their devices is always password protected.

d. Accept regular review and monitoring of their devices.

e. Protect their devices from loss, damage or theft and should report to relevant authorities when lost or stolen.

f. Allow remote wiping of data by the MCDA in case of theft or loss of the device or when no longer authorized to use the system.

g. Not disclose confidential information during employment and after separation.

5.0 SYSTEMS AND APPLICATIONS SECURITY

5.1 SYSTEMS ACQUISITION MAINTENANCE AND DECOMMISSIONING

Organizations acknowledge that it is their responsibility to protect information technology resources and their operating environment whether information is on site, in transit or hosted off-site. As such, this policy provides the overarching methodology and guiding principles to safeguard an organization in the acquisition, development, commissioning, maintenance and decommissioning of PFM Information Systems and applications. The purpose of this policy is to provide guidance on secure systems acquisition, development, commissioning, maintenance and decommissioning of PFM Information Systems in-line with the business needs and relevant procurement laws and regulations.

5.1.1 SCOPE

This policy covers the acquisition, development, commissioning, maintenance and decommissioning of all PFM Information Systems.

5.1.2 POLICY STATEMENT

Information security controls shall be an integral part of PFM systems through-out their entire life cycle.

5.1.3 GUIDELINES

5.1.3.1 Acquisition of systems shall conform to GoK ICT standards;

5.1.3.2 All vendor-supplied defaults for system passwords and other security parameters shall be changed;

5.1.3.3 Software development personnel shall be trained in writing secure code for their specific development environment and responsibilities to reduce dependency on contractors;

5.1.3.4 Appropriate code analysis tools shall be utilized to verify that secure coding practices are being adhered to for internally developed software.

5.1.3.5 Web application firewalls (WAFs) shall be deployed to protect all web based applications.

5.1.3.6 Escrow agreements shall be entered into for safeguarding of source code in the event the system is not fully owned by the MCDA;

5.1.3.7 Appropriate change control processes for PFM Information systems shall be put in place throughout the development lifecycle, coupled with

technical reviews of applications for any changes made after operating platform changes;

5.1.3.8 Changes to PFM Information Systems shall be controlled and documented;

5.1.3.9 Outsourced development shall be strictly controlled and monitored to ensure that information security controls are designed and implemented in the application;

5.1.3.10 System security testing shall be regularly conducted throughout system life cycle;

5.1.3.11 System acceptance testing and quality assurance shall be carried out for new systems, upgrades, and newer versions; and

5.1.3.12 The development team, shall incorporate technical staff with necessary capability for avoiding, finding, and fixing vulnerabilities.

5.1.4 MAINTENANCE OF PFM INFORMATION SYSTEMS

5.1.4.1 All applications shall be patched and updated regularly to ensure optimal and secure performance;

5.1.4.2 All equipment shall be maintained (preventive and corrective) regularly to ensure optimal and secure performance;

5.1.4.3 All active applications within PFM Information systems environment shall be monitored using appropriate tools;

5.1.4.4 MCDAs shall maintain separate environments for production and non-production/testing of PFM Information systems; and

5.1.4.5 MCDAs shall ensure regular backup of PFM Information systems as per the provided standards, guidelines and procedures.

5.1.5 DECOMMISSIONING OF PFM INFORMATION SYSTEMS

5.1.5.1 MCDAs shall define acceptable guidelines for identifying systems for decommissioning, in compliance with laid down Government disposal procedures;

5.1.5.2 MCDAs shall ensure the identified assets for decommissioning do not contain the application software, retain organizational data and ensure they are removed from active operating environment;

5.1.5.2 A data migration plan shall be developed that incorporates the following elements;

a. An impact analysis;

b. Issue of notification to service providers, users and customers;

c. Issue of notification of decommissioning to all relevant interfaces and interconnections;

d. Timeframe, plan and schedule;

e. Data integrity and validation checks before archiving;

f. Transfer or redeployment of equipment and other assets;

g. Transfer or cancellation of licenses;

h. Removal of obsolete equipment and software;

i. Removal of obsolete cables and termination equipment;

j. Removal of any emanation control equipment or security enhancements;

k. Return or safe disposal of any emanation control equipment or security enhancements;

l. Updates to systems configurations (switches, firewalls etc.)

m. Equipment and media sanitization including any cloudbased data & services

n. Any legal considerations for supply or service contract terminations

o. Asset register updates

p. Retraining or redeployment of support staff.

5.2 APPLICATION PROGRAMMING INTERFACES (APIs) AND INTEROPERABILITY

Interoperability refers to the ability of systems to connect and communicate with one another readily, even if they were developed on different platforms. Being able to exchange information between applications, databases, and other computer systems is crucial for seamless operations. Application Programming Interfaces (APIs) facilitate interoperability by enabling applications to exchange data and functionality easily and

securely. Therefore, there is need to guide secure and effective integration of Public Financial Management Information Systems with other systems.

5.2.1 SCOPE

This covers the use of APIs to integrate PFM Information Systems with other relevant Information Systems.

5.2.2 POLICY STATEMENT

Integration of PFM Information Systems with other relevant systems shall be done in adherence to this policy and the given standards, guidelines and procedures.

5.2.3 GUIDELINES

When implementing APIs and designing interoperability of systems MCDAs shall ensure:

5.2.3.1 Data formats are in accordance with the targeted systems in order to avoid transmission errors;

5.2.3.2 Request parameters of relevant error messaging are validated to defend against injection attacks;

5.2.3.3 Proper authentication and authorization is enforced to ensure that data is from authorized parties only;

5.2.3.4 Controls are established to guard against manipulation of data in active transactions and attempts to alter transactions should trigger alerts and be logged and audit trails maintained;

5.2.3.5 Digital signatures are used to safeguard against nonrepudiation of transactions;

5.2.3.6 Data is encrypted using the latest technology when on transit and at rest; and

5.2.3.7 All PFM Information Systems are developed and integrated as per the Government ICT Standards on information security

5.3 VIRTUALIZATION

Virtualization is the process of running a virtual instance of a computer system in a layer abstracted from the actual hardware. Most commonly, it refers to running multiple operating systems on a computer system simultaneously. This allows computing resources to be used more efficiently by a number of different users or applications with different needs.

5.3.1 SCOPE

This covers PFM Information systems deployed and operating in virtualized environments.

5.3.2 POLICY STATEMENT

To evaluate, monitor and manage security within a virtual environment in PFM Information Systems.

5.3.3 GUIDELINES

In the deployment of virtualization technology MCDAs shall:

5.3.3.1 Ensure the security of each virtual machine;

5.3.3.2 Secure virtual networks from attacks and vulnerabilities that may surface from the underlying physical environment;

5.3.3.3 Ensure guest operating system is isolated from the host operating system;

5.3.3.4 Ensure both the host and virtual environment are only accessed by authorized user(s);

5.3.3.5 Ensure virtualization software is up-to-date with vendor patch releases;

5.3.3.6 Ensure access and visibility between the guests hosted within the host operating systems shall be restricted; and

5.3.3.7 Routinely inspect and monitor the virtualization environment, perform audits to flag suspicious configurations and communication between the guests.

6. 0 COMMUNICATION SECURITY

This stipulates how the PFM Information Systems will handle communication between its internal and external stakeholders. The purpose of this policy is to ensure the protection of information in networks and its supporting information processing facilities, and maintain the security of information transferred within the PFM Systems and with any external entity in a manner consistent with current best practices to ensure confidentiality, integrity, availability, accuracy, authenticity, utility and possession.

Communication Security entails; Network Security, Wireless Security, Electronic Messaging, Information Sharing and Agreement on Information Transfer that are in many ways inter-related.

6.1 NETWORK SECURITY

Network Security is a set of rules and configurations designed to protect the integrity, confidentiality, accessibility accuracy, authenticity, utility and possession of computer networks and data using both software and hardware technologies. Computer networks are integral part in communication and sharing of resources, data and applications. Network Security guides on use, protection and security of information in networks for PFM Information Systems.

6.1.1 SCOPE

Network security covers all aspects of computer networks infrastructure, configurations, management and their use.

6.1.2 POLICY STATEMENT

Network security directs the processes and procedures by which PFM Information systems ensure a secure method of connectivity and provide guidelines for the use of network and computing resources associated with the network connection.

6.1.3 GUIDELINES

To ensure that a secure method of connectivity is provided for the use of network and computing resources associated with the network connection the MCDAs shall;

6.1.3.1 Ensure network operations related passwords e.g. for switches and routers are securely stored;

6.1.3.2 Ensure regular scans are performed from outside each trusted network perimeter to detect any unauthorized connections which are accessible across the boundary;

6.1.3.3 Deny communications with known malicious Internet Protocol (IP) addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries;

6.1.3.4 Deny communication over unauthorized ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries;

6.1.3.5 Deploy network-based Intrusion Detection Systems (IDS) to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries;

6.1.3.6 Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries;

6.1.3.7 Enable the collection and monitoring of network flows and logging data on network boundary devices;

6.1.3.8 Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections;

6.1.3.9 Require all remote login access to their network is encrypted;

6.1.3.10 Maintain standard, documented security configurations for all authorized network devices;

6.1.3.11 Compare all network device configurations against approved security configurations defined for each network device in use and alert when any deviations are discovered;

6.1.3.12 Install the latest stable version of any security related updates on all network devices;

6.1.3.13 Manage network devices using multi-factor authentication and encrypted sessions where possible;

6.1.3.14 Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system;

6.1.3.15 Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed;

6.1.3.16 Place application layer firewalls in front of any critical network segments to verify and validate the traffic going to the network. Any unauthorized traffic should be blocked and dropped and source logged where necessary;

6.1.3.17 Automatically disconnect users connected through a VPN after prescribed time of inactivity;

6.2 WIRELESS SECURITY

A wireless network is a computer network that allows devices to stay connected to the network but roam untethered to any wires. This includes all wireless communication devices capable of transmitting packet data (for example, personal computers, wireless phones, smart phones, etcetera) connected to any of the PFM Information Systems networks.

6.2.1 SCOPE

Wireless security covers all aspects of wireless networks infrastructure, configurations, management and use in PFM Information Systems.

6.2.2 POLICY STATEMENT

This policy shall guide on access and management of wireless networks and computing resources associated with connection of PFM Information Systems.

6.2.3 GUIDELINES

MCDAs shall:

6.2.3.1 Ensure all wireless access points are registered, have data encryption methods, have multi-factor authentication method in accordance with GOK ICT Network Standard and Security Standard;

6.2.3.2 Maintain an inventory of authorized wireless access points connected to the wired network;

6.2.3.3 Configure network vulnerability scanning tools to monitor, detect and alert on unauthorized wireless access points connected to the wired network;

6.2.3.4 Disable wireless access on devices that do not have a business purpose for wireless access or pose a risk in facilitating ad-hoc wireless connections (computer to computer), by-passing network controls;

6.2.3.5 Leverage on wireless encryption standards for data in transit;

6.2.3.6 Ensure that wireless networks use authentication protocols; and **6.2.3.7** Scan wireless devices for malware before admission to the network.

6.3 ELECTRONIC MESSAGING

Electronic messaging also referred to as electronic mail is an interactive, computer-driven technology that facilitates two-way interpersonal communication among individuals or groups. This provides guidance and direction for electronic messaging such as e-mail, chat; containing confidential and/or protected information that may be passed through PFM Information systems.

6.3.1 SCOPE

Electronic Messaging covers all aspects of electronic messaging as used in the PFM Information Systems.

6.3.2 POLICY STATEMENT

Security controls shall be established to protect electronic messaging from unauthorized access, modifications or denial of service. Electronic messages on PFM Information systems are considered organization's information assets and as such, the PFM Information Systems owners shall have right to access, control and examine such messages on need basis.

6.3.3 GUIDELINES

6.3.3.1 Electronic messages containing confidential and/or protected information that may travel across external networks shall utilize a physical or logical encryption mechanism to ensure the confidentiality and integrity of the information;

6.3.3.2 Protected and/or confidential information shall not be entered in the subject line of any electronic message.

6.3.3.3 PFM Information systems users shall not provide their login ID or password to another person or vendor due to potential security risks;

6.3.3.4 Auto-forwarding emails containing protected information to any external mail service shall not be permitted;

6.3.3.5 PFM Information systems users shall not subject their official email accounts for private communication;

6.3.3.6 MCDAs shall install anti-malware software that shall auto-scan attachments before they are opened by users;

6.3.3.7 When dealing with external stakeholders for official communication,

a. PFM Information System users shall only use official emails

b. Avoid confidential information in subject line;

6.3.3.8 All PFM Information Systems users shall employ electronic messaging practices in accordance with GoK ICT Security Standard.

6.4 INFORMATION SHARING

PFM Information Systems place a strong emphasis on the need to share information across organizational and professional boundaries, in order to ensure effective co-ordination and integration of services. This calls for the embedding of security and confidentiality in relation to all information held by PFM Information Systems for strengthening the legislation and guidance in this area in particular through the Data Protection Act, 2019.

Information sharing can take the form of:

a. A reciprocal exchange of data;

b. One or more PFM Information Systems providing data to a third party or parties;

c. Several PFM Information Systems pooling information and making it available to each other as well as third parties; and

d. Exceptional, one-off disclosures of data in unexpected or emergency situations.

6.4.1 SCOPE

This covers all aspects of information sharing in PFM Information Systems while ensuring security of the information.

6.4.2 POLICY STATEMENT

It is important that we protect and safeguard information in order to comply with the law and to provide assurance to the public.

6.4.3 GUIDELINES

6.4.3.1 The PFM Information Systems Users shall adhere to retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant Government Policies and regulations;

6.4.3.2 The PFM Information Systems Users shall adhere to controls and restrictions associated with using communication facilities, e.g.

automatic forwarding of electronic mail to external mail addresses;

6.4.3.3 The PFM Information Systems Users shall take appropriate precautions not to reveal confidential information; and

6.4.3.4 PFM Information Systems owners shall develop procedures to safeguard transfer of information in accordance with GoK ICT Security Standard.

6.5 AGREEMENTS ON INFORMATION TRANSFER

The management of the transmission, dispatch and control should be notified to the relevant parties. A mutual agreement to protect the information transmitted should be created. Agreements should address secure transfers between the organization and outside parties of business information. This provides guidance on management of the transmission, dispatch and control of information undertaken through the PFM Information Systems.

6.5.1 SCOPE

This covers all agreements on information transfer as executed in the PFM Information Systems.

6.5.2 POLICY STATEMENT

Formal controls based on the criticality of information shall be defined to protect the transfer of information through the use of communication facilities. Transfer of confidential information shall be appropriately protected. Prior to the transfer of information with external organization, a formal and an appropriate SLA with an adequate level of security controls shall be defined.

6.5.3 GUIDELINES

6.5.3.1 All users shall manage the creation, storage, amendment, copying and deletion or destruction of data (in electronic and paper form) in a manner which is

consistent with Government policies, and which control and protect the confidentiality, integrity and availability of such data;

6.5.3.2 Information Asset Owners shall ensure appropriate mechanisms are implemented and followed to protect transfer of their information;

6.5.3.3 Agreements on information transfer should cover, but not be limited to:

- **a.** Management responsibilities.
- **b.** Manual and electronic exchanges.
- **c.** Sensitivity of the critical information being exchanged.
- **d.** Protection requirements.
- **e.** Notification requirements.
- **f.** Packaging and transmission standards.
- **g.** Courier identification.
- **h.** Responsibilities and liabilities.
- **i.** Data and software ownership.
- **j.** Protection responsibilities and measures.
- **k.** Encryption requirements.

7.0 INFORMATION SECURITY RISK MANAGEMENT

Risk management is the process of identifying vulnerabilities and threats to the information resources used by PFM Information systems in achieving its objectives and deciding what countermeasures to take in reducing risk to an acceptable level. The purpose is to empower the MCDAs to perform periodic information security risk assessment to determine areas of vulnerability, and to initiate appropriate remedies.

7.1.1 SCOPE

Information Security Risk Management shall be conducted on all PFM Information Systems operating environments including but not limited to infrastructure, procedures and personnel.

7.1.2 POLICY STATEMENT

The MCDAs operating PFM Information Systems shall develop an information security risk management plan to provide a structured way of risk identification, analysis, and implementation of appropriate risk management procedures in consideration of existing legal and regulatory frameworks relevant to the MCDAs.

7.1.3 GUIDELINES

7.1.3.1 Information security risk management shall be undertaken as part of the MCDA Risk Management;

7.1.3.2 The execution, development and implementation of remediation programs shall be a joint responsibility of the Accounting Officer and the system owners;

7.1.3.3 System owners shall cooperate fully with risk assessment being conducted on systems/processes for which they are accountable for;

7.2 INFORMATION ASSET MANAGEMENT

Information asset refers to any device or media used to store information in any form. Information asset management is therefore the effective management, control and protection of information assets within the MCDAS. The purpose is to provide guidance in the management of information assets within PFM Information systems.

Information assets include**;**

- **a.** operating systems

b. infrastructure

c. applications

d. records

e. Data and information

f. ICT hardware

7.2.1 SCOPE

This covers acquisition, maintenance and disposal of information assets in the PFM Information Systems operation environment.

7.2.2 POLICY STATEMENT

Information assets shall be acquired, operated, maintained and disposed in adherence to the information security standards and guidelines.

7.2.3 GUIDELINES

7.2.3.1 An inventory of all information assets shall be implemented and maintained for PFM Information Systems;

7.2.3.2 Access restrictions and classifications shall be defined and periodically reviewed to critical assets;

7.2.3.3 Information assets shall be maintained regularly as per the manufacturers' recommendations;

7.2.3.4 Proper security of information assets shall be maintained when the asset is decommissioned, disposed or destroyed;

7.2.3.5 Information system owners shall define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies;

7.2.3.6 Rules for the acceptable use of information and associated assets with information and information processing facilities shall be identified, implemented and documented;

7.2.3.7 Officers and external users shall return all MCDAs information assets in their possession upon termination of their employment, contract or agreement;

7.2.3.8 In cases where officers or external user purchase the organization's information assets or equipment procedures shall be followed to ensure that all relevant

information is transferred to the MCDAs and securely erased from the equipment;

7.2.3.9 In cases where officers or external users have knowledge that is important to ongoing operations, that information shall be documented and transferred to the MCDAs;

7.2.3.10 The MCDAs shall control copying of sensitive information;

7.2.3.11 MCDAs shall implement appropriate controls when the information asset is scheduled for maintenance;

7.2.3.12 Before putting the information asset back into operation after maintenance, it shall be inspected to ensure that it has not been tampered with;

7.2.3.13 Formal procedures shall be documented for secure disposal of media and assets to minimize the risk of confidential information leakage to unauthorized persons;

7.2.3.14 All users shall be made aware of the security requirements and procedures for protecting unattended information assets, as well as their responsibilities for implementing information security guidelines; and

7.2.3.15 MCDAs shall ensure storage of ICT assets in accordance with manufacturers' specifications.

7.3 INFORMATION CLASSIFICATION AND SHARING

Information classification is a process in which MCDAs assess the data that they hold and the level of protection that it should be given while maintaining confidentiality and integrity before dissemination. The purpose of this policy is to help the MCDAs manipulate, track and analyze individual pieces of information.

Information classification scheme shall be based on four levels as follows:

- Disclosure causes no harm to the MCDA;
- Disclosure causes minor embarrassment or minor inconvenience to operations, personnel of the MCDA;
- Disclosure has a significant short term impact on operations, strategic objectives, personnel and reputation; and
- Disclosure has a serious impact on long-term strategic objectives operations, personnel and reputation of the MCDAs.

7.3.1 SCOPE

There should be an information classification scheme that applies across all PFM Information Systems in the MCDAs, which is used to determine varying levels of confidentiality, availability and integrity of information.

7.3.2 POLICY STATEMENT

It shall apply to all custodians & administrators of PFM Information Systems users and other authorized affiliates and failure to comply may result to sanctions.

7.3.3 GUIDELINES

7.3.3.1 MCDAs shall classify information as per the scheme above. It shall classify; information stored in physical form, electronic form and communications medium;

7.3.3.2 Information shall be classified in line of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification;

7.3.3.3 MCDAs shall ensure protection of temporary or permanent copies of information to a level consistent with the protection of the original information;

7.3.3.4 MCDAs shall ensure clear marking of all copies of media for the attention of the authorized recipient;

7.3.3.5 MCDAs shall document and implement the following guidelines to protect media containing information being transported:

- **a.** Reliable and authorized couriers shall be used;
- **b.** Packaging shall be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications; and
- **c.** Logs shall be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.

7.4 ACCEPTABLE USE POLICY

This policy regulates the use of all ICT facilities owned, leased or hired by MCDAs, and it applies to every employee, contractors and third parties who are granted access to PFM Information System. MCDAs reputation, and the effectiveness and efficiency of what it does, can be put at considerable risk if users, contractors, and third-parties authorized to

access, handle or use MCDAs information – fail to maintain proper standards and controls in the way they manage information security. The MCDAs are responsible for maintaining the security and integrity of their information and communications systems.

7.4.1 SCOPE

This Policy is applicable to information/data assets including, but not limited to, hard copies of documents, electronic data, images, computer equipment, network or data communication equipment, computer programs, procedures and support software, data storage devices and media.

7.4.2 POLICY STATEMENT

All users shall be required to adhere to the laid down controls to mitigate security risks regarding information/data that they access, handle or use, and report information security breaches to relevant Authorities.

7.4.3 GUIDELINES

7.4.3.1 ICT resources shall only be used for legitimate purposes related to the activities of the MCDAs. When using ICT resources, users must uphold and promote the highest standards of ethical and professional conduct. Inappropriate use of ICT resources shall result in disciplinary action up to and including dismissal.

7.4.3.2 Users are responsible for the safekeeping of any ICT equipment provided to them (like laptops or mobile phones). Any loss of such equipment must be reported to the relevant authorities.

7.4.3.3 Use of ICT resources must comply with applicable laws.

7.4.3.4 Use of ICT resources shall be monitored to check adherence to this security policy, standards and guidelines.

7.4.3.5 Visiting sites that contain illegal material or in violation of MCDAs policies or local laws is prohibited;

7.4.3.6 Using the Internet to send offensive or harassing material to other people is prohibited;

7.4.3.7 Employees shall not be allowed to perpetrate any form of fraud or illegal activities;

7.4.3.8 Downloading or storing unlicensed software or any copyrighted materials belonging to third parties is prohibited, unless covered or permitted under commercial agreement or other such license;

7.4.3.9 Performing any form of hacking including but not limited to reconnaissance, scanning, and trying to gain unauthorized access into MCDAs information assets is prohibited;

7.4.3.10 Intentionally introducing malicious code, including, but not limited to viruses, worms, Trojan horses, e-mail bombs, spyware, adware and key loggers is prohibited.

7.4.3.11 Effecting security breaches or disruptions of network communication is prohibited. Security breaches include but are not limited to accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access.

7.4.3.12 Unauthorized changing of the configuration settings or naming standards of the information assets is prohibited.

7.4.3.13 Spamming is prohibited.

7.4.3.14 Forging, misrepresenting, obscuring, suppressing or replacing a user identity on any electronic communication to mislead the recipient about the sender is prohibited.

7.4.3.15 Revealing confidential information about MCDAs in a personal online posting, upload or transmission is prohibited;

7.4.3.16 Conducting business on personal or non- MCDAs that results in the storage of proprietary information on personal or non-MCDA controlled environments, including devices maintained by a third party with whom MCDAs do not have a contractual agreement, is prohibited.

7.4.3.17 Using any of MCDAs ICT facilities for personal commercial gain (including advertising) is prohibited;

7.5 BUSINESS CONTINUITY MANAGEMENT

Business Continuity Management provides a framework for advanced planning and preparation of MCDAs to maintain PFM Information systems to continue offering critical services or quick resumption in the event of disruption. This encompasses Business Continuity Planning, Disaster Recovery Planning and Back-up and Recovery Planning.

7.5.1 SCOPE

It covers all the PFM Information Systems resources and personnel that support critical business processes.

7.5.2 POLICY STATEMENT

The custodians/administrators of PFM Information Systems shall develop, implement, maintain and document Business Continuity Plans, Disaster Recovery Plans, Data Backup and Recovery Plans as per GoK ICT standards and guidelines.

7.5.3 GUIDELINES

7.5.3.1 BUSINESS CONTINUITY PLANNING (BCP)

MCDAs shall develop, implement and maintain Business Continuity Plans (BCPs) in adherence to GoK ICT Standards and guidelines. The BCPs must be documented and tested against the business functions and applications to confirm continuance and resiliency of critical services in the event of a disruption;

i. MCDAs shall develop, implement and maintain business continuity plan. Information security requirements shall be determined when planning for business continuity and disaster recovery.

ii. The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of business continuity.

iii. MCDAs shall ensure that:
   - Adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;
   - A business continuity team is constituted to compile a business continuity plan and manage business disruption;
   - Documented plans, response and recovery procedures are developed and approved;
   - Incident response personnel with the necessary responsibility, authority and competence to manage an incident are nominated;

iv. MCDAs shall identify business requirements for the availability of information systems.

v. MCDAs shall conduct a business impact analysis to identify time sensitive or critical business functions and processes and the resources that support them.

vi. MCDAs shall organize a business continuity team and compile a business continuity plan to manage a business disruption.

vii. MCDAs shall conduct training for the business continuity team and testing and exercises to evaluate recovery strategies and the plan

7.5.3.2 DISASTER RECOVERY PLANNING (DRP)

The following contingency plans must be created:

i. Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?

ii. Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.

iii. Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.

iv. Criticality of Service List: List all the services provided and their order of importance.

It also explains the order of recovery in both short-term and long-term timeframes.

v. Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.

vi. Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.

vii. Mass Media Management: Who is in charge of giving information to the mass media?

viii. Guidelines on what data is appropriate to be provided.

x. Management should set aside time to test implementation of the disaster recovery plan. Tabletop exercises should be conducted quarterly.

xi. The plan, at a minimum, should be reviewed an updated on an annual basis.

7.5.3.3 BACKUP AND RESTORATION PLAN

MCDAs shall develop, implement and maintain Back-up and Restoration Plans in adherence to GoK ICT Standards and guidelines. The plans must be tested, audited and documented regularly to ensure that they meet the requirements of the business continuity management.

i. MCDA shall develop a backup policy to define the organization's requirements for backup of information, software and systems;

ii. When designing a backup plan, the following items shall be taken into consideration

iii. Accurate and complete records of the backup copies and documented restoration procedures;

iv. The extent (e.g. full or differential backup) and frequency of backups;

v. Criticality of the information for the continuity of operations of the organization;

vi. The backups shall be stored in a remote location, at a sufficient physical distance.

vii. Backup information shall be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site;

viii. Backup media shall be regularly tested to ensure that they can be relied upon for emergency use when necessary; this shall be combined with a test of the restoration procedures and checked against the restoration time required;

ix. Testing the ability to restore backed-up data shall be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss;

x. In situations where confidentiality is of importance, backups shall be protected by means of encryption;

xi. Operational procedures shall monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups;

xii. Backup arrangements for individual systems and services shall be regularly tested to ensure that they meet the requirements of business continuity plans.

xiii. The retention period for essential business information shall be determined, taking into account any requirement for archive copies to be permanently retained.

7.6 THREAT AND VULNERABILITY MANAGEMENT

It is the recurring practice of identifying, assessing, classifying, remediating, and mitigating security weaknesses together with fully understanding root cause analysis to address potential flaws in the PFM operating environment. The purpose is to provide guidance in the remediation of security weaknesses in PFM Information systems.

7.6.1 SCOPE

This covers the identification, assessment, classification, remediation and mitigation of information security weaknesses in PFM Information systems.

7.6.2 POLICY STATEMENT

MCDAs shall regularly identify, assess, classify, remediate and mitigate security weaknesses and their root causes in PFM Information Systems.

7.6.3 GUIDELINES

7.6.3.1 MCDAs shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required;

7.6.3.2 Timelines shall be defined to react to notifications of potentially relevant vulnerabilities;

7.6.3.3 Procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks shall be developed;

7.6.3.4 Regular reviews of the software and data content of systems supporting critical business shall be conducted and the presence of any unapproved files or unauthorized amendments shall be formally investigated;

7.6.3.5 Once a potential technical vulnerability has been identified, the MCDAs shall identify the associated risks and the actions to be taken; such actions could involve patching of vulnerable systems or applying other controls;

7.6.3.6 MCDAs shall carry out installation and regular updates of antimalware software;

7.6.3.7 MCDAs shall define a procedure to address the situation where vulnerability has been identified but there is no suitable countermeasure;

7.6.3.8 Patches shall be tested and evaluated before they are installed on a production system to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls shall be considered, such as:

- **a.** Turning off services or capabilities related tothe vulnerability;
- **b.** Adapting or adding access controls, e.g. firewalls, at network borders;
- **c.** Increased monitoring to detect actual attacks; and
- **d.** Raising awareness of the vulnerability to the relevant teams.

7.6.3.9 An effective technical vulnerability management process shall be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur;

7.6.3.10 Use of unauthorized software is prohibited and MCDAs should implement controls that prevent or detect the use of unauthorized software and suspected malicious websites.

8.0 HUMAN RESOURCES SECURITY

8.1 INTRODUCTION

This is to provide Public Financial Management Reforms Information Systems users with guidelines and requirements regarding human resources security and its objective is to ensure that all employees (including contractors and any user of sensitive data) are qualified for and understand the roles and responsibilities of their duties and that access is removed once employment is terminated. Proper information security practices should be in place to ensure that employees, contractors and third-party users understand their responsibilities and are suitable for their assigned roles.

These practices can reduce the risk of theft, fraud or misuse of facilities. Specific security practices include:

a. Security responsibilities should be addressed prior to employment in adequate job descriptions, terms and conditions of employment;
b. All candidates for employment, contractors and third-party users should be adequately screened especially for sensitive jobs; and
c. All stakeholders and other users of information processing facilities should sign an agreement on their security roles and responsibilities, including the need to maintain confidentiality;

8.1.1 SCOPE

This applies to all stakeholders accessing all operating PFM data and systems, during the time of active engagement.

8.1.2 POLICY STATEMENT

MCDA shall ensure all stakeholders who are involved in PFM Information Systems and data are aware of understand and fulfill their responsibilities in regards to information security.

8.1.3 GUIDELINES

MCDAs shall manage human resource security in the following ways:

8.1.3.1 Provide management direction and support for information security in accordance with business requirements, this policy and other relevant laws and regulations;

8.1.3.2 Responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the officer and enforced;

8.1.3.3 New system users shall be trained on system use;

8.1.3.4 Ensure that all stakeholders are aware of and fulfill their information security responsibilities and by signing a non-disclosure agreement

8.1.3.5 Protect the MCDAs interests as part of the process of changing or terminating employment**.**

8.1.3.6 MCDA shall have contractual agreements that follow stipulated standards and guidelines with their employees and contractors that reflect the organization's policies for information security.

8.2 BACKGROUND SCREENING

This is a process used by MCDAs to verify that an individual is who they claim to be and thus provides an opportunity to check and confirm the validity of someone's criminal record, education, employment history, and other activities from their past and will typically take place any time MCDAs deems necessary. A variety of methods will be used to complete these checks including a comprehensive database search and personal references.

8.2.1 POLICY STATEMENT

There shall be a pre-employment and pre-contractual procedure done to help reassure organizations that they are hiring trustworthy individuals;

8.2.2 GUIDELINES

8.2.2.1 MCDAs shall conduct background verification checks on all candidates for employment in accordance with relevant laws, regulations and ethics;

8.2.2.2 The screening shall be proportional to the MCDAs requirements, the classification of the information to be accessed and the perceived risks;

8.2.2.3 Internal promotions that involves the person accessing mission critical assets shall also attract further and more detailed vetting.

8.3 IN-SERVICE

8.3.1 POLICY STATEMENT

MCDAs shall ensure that all stakeholders are aware of, understand, and fulfill their responsibilities in regards to information security.

8.3.2 GUIDELINES

8.3.2.1 All MCDAs staff shall conform to the terms and conditions of employment, which includes information security and appropriate methods of working; and

8.3.2.2 MCDAs shall be provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing").

8.3.2.3 There shall be a formal and communicated disciplinary process in place to take action against officers who have committed an information security breach.

8.4 TERMINATION OR CHANGE OF RESPONSIBILITIES

8.4.1 POLICY STATEMENT

MCDAs shall ensure that the process of termination or change of responsibilities will be communicated appropriately to all relevant stakeholders;

8.4.2 GUIDELINES

8.4.2.1 To prevent unauthorized access to sensitive information, access shall be revoked immediately upon termination/change of a user;

8.4.2.2 Termination or change of responsibilities shall be communicated appropriately to all relevant stakeholders;

8.4.2.3 All access rights issued shall be disabled or reassigned in accordance to the access control section of this policy.

8.5 INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

8.5.1 POLICY STATEMENT

The information security awareness program should aim to make all stakeholders aware of their responsibilities for information security and the means by which those responsibilities are discharged.

8.5.2 GUIDELINES

8.5.2.1 Officers in MCDAs handling information security shall be regularly trained on professional courses pertaining to information security in adherence to the GoK ICT Standard on Human Capital and Workforce Development Standard;

8.5.2.2 MCDAs through the information security steering committees shall plan and conduct customized information security sensitization programme annually according to employees' roles in the organization;

8.5.2.3 An assessment of the employees' understanding shall be conducted at the end of an awareness sensitization course to test knowledge retention and understanding.

9.0 OPERATIONAL SECURITY

Security of PFM Information Systems is paramount hence MCDAs shall ensure correct and secure operations of information processing facilities. Operational security includes access control, cloud security, change management, user account management and password policy.

9.1 ACCESS CONTROL

The MCDAs shall implement this access control policy based on their business processes and information Security requirements. This outlines controls placed on both physical access to the computer system and to the software in order to limit access to computer networks and data. The purpose of this policy is to provide guidance on the design of access controls to minimize potential threats to PFM Information Systems resulting from unauthorized use of resources.

9.1.1 POLICY STATEMENT

Access to PFM Information systems and resources shall be granted based on the principle of least privilege and the need-to-know basis.

9.1.2 GUIDELINES

9.1.2.1 Access rights and privileges to PFM Information systems shall be assigned based on user's roles and responsibilities on the respective systems and applications;

9.1.2.2 User access passwords shall conform to the section on passwords in this policy (Clause 9.5);

9.1.2.3 All PFM Information Systems shall have audit logs to track users' activity and be monitored regularly;

9.1.2.4 Remote access to the PFM Information systems shall be allowed through an authorized secure connection e.g. VPN;

9.1.2.5 Periodic audits of access controls and user rights shall be conducted to ensure they are working as expected;

9.1.2.6 MCDAs shall ensure periodical identification, disabling and retire inactive user IDs;

9.1.2.7 Access to program source codes shall be restricted to authorized personnel and shall be written in English language.

9.2 CLOUD SECURITY

Cloud computing is the on-demand availability of computer data storage and computing resources without direct active management by the user. This mainly defines data centers available to many users over the Internet. The purpose of this policy is to provide guidance for secure acquisition and deployment of cloud based PFM Information Systems.

9.2.1 SCOPE

This policy covers the acquisition and deployment of cloud based PFM Information Systems.

9.2.2 POLICY STATEMENT

In order to enhance efficiency, cloud computing shall be adopted for PFM Information Systems in conformity with GoK ICT Standard on information security and applicable legislation.

9.2.3 GUIDELINES

The following guidelines shall apply to the acquisition and management of cloud computing solutions:

9.2.3.1 Adequate safeguards shall be put in place to secure authentication, authorization and access management functions that are suitable for MCDAs;

9.2.3.2 MCDAs shall adhere to the GoK ICT Standard on Cloud Computing during design, installation and management of cloud computing infrastructures;

9.2.3.3 Contracts with cloud service providers shall include:

- **a.** An exit plan especially requiring the cloud provider to provide a way to extract data easily and economically.
- **b.** A requirement for data sanitization, electronic and physical access rights be revoked from the cloud provider, assets provided to the provider returned and data securely purged upon separation.
- **c.** Non-Disclosure Agreement before provisioning any cloud service.
- **d.** Full disclosure in case of breaches to regulated information.
- **e.** Ownership of Government data.
- **f.** Any other standard intellectual property clauses relevant to the service.
- **g.** Privacy legislation compliance.

h. Service Level Agreements to meet availability, performance and disaster recovery requirement service management processes.

i. Audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.

j. A clear process documenting the responsibilities of each party with respect to extracting and destroying data.

9.2.3.4 Request proof of independent security reviews and certification reports that meet the MCDA compliance requirement.

9.3 CHANGE MANAGEMENT

Change management is an ICT practice designed to minimize disruptions to ICT services while making changes to critical systems and services. The purpose of this policy is to guide the process of instituting changes in the PFM Information systems operational environment in order to ensure that they are carried out in a planned manner to minimize negative impact to services.

9.4.1 SCOPE

This policy covers all changes in the implementation of new ICT infrastructure, systems and related technologies.

9.4.2 POLICY STATEMENT

Changes to configurations, systems, applications or equipment that affect PFM Information systems operational environment shall follow the appropriate change management procedures in this policy and GoK ICT Standards to minimize adverse impacts of the changes to operations.

9.4.3 GUIDELINES

9.4.3.1 MCDAs shall ensure identification and recording of significant changes that affect PFM Information systems;

9.4.3.2 All changes shall be planned, tested and communicated to all relevant stakeholders;

9.4.3.3 MCDAs shall ensure that assessment of the potential impacts, including information security impacts of changes in PFM Information systems are documented;

9.4.3.4 Changes requested by users shall contain sufficient information to enable the evaluation of the potential risks and benefits;

9.4.3.5 A roll-back plan shall be developed and tested before a change is implemented;

9.4.3.6 MCDAs shall ensure changes are effected without disrupting service delivery;

9.4.3.7 Users shall be notified of the changes made on the PFM Information systems and taken through training on the new operational processes impacted by a change in PFM Information Systems.

9.4.3.8 Users shall review and accept completion of the changes in readiness for transition to production environment and the review shall be documented;

9.4.3.9 An audit log of all relevant information on the changes shall be retained.

9.5 USER ACCOUNT MANAGEMENT

There is need to carefully manage all user accounts, especially those accounts that have administrative rights on the PFM Information Systems. The purpose of this policy is to establish the rules for the creation, use, monitoring, control and retirement of user accounts and to ensure that all approved users are created using the principle of least privilege.

9.5.1 SCOPE

The policy covers creation, use, monitoring, control and retirement of user accounts accessing PFM Information systems operation environment.

9.5.2 POLICY STATEMENT

All authorized users of PFM Information systems shall have accounts created for them in accordance with this policy.

9.5.3 GUIDELINES

9.5.3.1 Heads of section should formally make requests for user account creation for their staff to the Accounting Officer for approval;

9.5.3.2 All user accounts must be uniquely created and identifiable;

9.5.3.3 User accounts that are unused or inactive for thirty days shall be automatically locked or disabled;

9.5.3.4 Users shall be granted privileges that are commensurate with their roles and responsibilities in the PFM Information systems;

9.5.3.5 All users shall have account management instructions, documentation, training and authorization;

9.5.3.6 All users must refrain from abuse of privilege;

9.5.3.7 All accounts access must meet the PFM Information Systems Password Policy;

9.5.3.8 In cases where a system has only one administrator, a password escrow procedure must ensure that someone other than the administrator can gain access to the administrator account in an emergency via use of securely kept password envelopes;

9.5.3.9 When Special Access accounts are requested for internal or external Audit, software development, software installation, or other defined need, they must be:

- **a.** authorized;
- **b.** created with a specific expiration date;
- **c.** Retired when work is complete.

9.5.3.10 The competences of users with privileged access rights shall be reviewed regularly in order to verify if they are in line with their duties.

9.6 PASSWORD POLICY

Passwords are the primary means of providing user access to system resources. To prevent information theft, users must ensure the confidentiality of all passwords used to connect to PFM Information systems. The purpose of this policy is to establish guidelines for creation of strong passwords, the protection of those passwords and the frequency of change.

9.6.1 SCOPE

The policy covers all users who access the PFM Information systems.

9.6.2 POLICY STATEMENT

All users accessing the PFM Information Systems shall be authenticated using a password.

9.6.2 GUIDELINES

9.6.2.1 Passwords shall be used on all PFM automated information systems to uniquely identify individual users;

9.6.2.2 Password complexity design shall be incorporated in all PFM Information systems to include the following: have at least 6 characters, upper case, lower case, special characters and numbers;

9.6.2.3 Passwords shall not be shared amongst users, neither be generic;

9.6.2.4 An intruder lock-out feature shall suspend accounts after three invalid attempts to log on; action by an administrator after user verification is required to reactivate the account;

9.6.2.5 Passwords shall expire after every 90 days;

9.6.2.6 Password should not be dictionary words;

9.6.2.7 Passwords shall not be portions of associated account names (e.g. user ID, log-in name, personal information);

9.6.2.8 Passwords shall not be character strings (e.g. abc or 123);

9.6.2.9 Passwords shall not be simple keyboard patterns (e.g. QWERTY, asdf);

9.6.2.10 Users are responsible for the security of their password(s) and shall be accountable for any misuse;

9.6.2.11 Incidents where accounts are suspected to have been compromised shall be reported to the system administrator;

9.6.2.12 Any default passwords must be changed on all systems prior to connection to any network including pre-deployment testing;

9.6.2.13 Systems should be configured to lock a session after a pre-determined time of inactivity;

9.6.2.14 Vendor or service accounts will be retired from computer systems prior to deployment and new passwords shall be implemented on all systems immediately upon installation at PFM ICT facilities by the system administrator;

10.0 PHYSICAL AND ENVIRONMENTAL SECURITY

PFM Information systems are supported by several Information resources comprised of software and hardware. The protection of these resources is paramount towards ensuring that they continue to deliver on their intended objectives.

This policy provides the guidance for the physical protection of ICT resources within the PFM Information Systems environment.

10.1 SCOPE

This policy covers all information processing facilities for PFM Information Systems.

10.2 POLICY STATEMENT

MCDAs shall ensure protection of critical and sensitive PFM Information Systems information processing facilities.

10.3 GUIDELINES

The following guidelines shall apply with regards to physical security of ICT resources:

10.3.1 Removable media (flash disks, portable hard drives) should be securely stored when not in use and kept away from environmental hazards;

10.3.2 MCDAs shall ensure installation of clean power to protect PFM ICT equipment from damage;

10.3.3 Employees shall not take ICT equipment out of the offices without an approved gate pass duly authorized by their Head of Department or as per organizational procedures;

10.3.4 Employees should exercise care to safeguard the valuable electronic equipment assigned to them failure to which they shall be held accountable;

10.3.5 MCDAs shall ensure ICT facilities are hosted within physically and environmentally secured areas;

10.3.6 MCDAs shall deploy surveillance and monitoring mechanisms to cover all critical ICT equipment installations;

10.3.7 MCDAs shall restrict access to critical ICT installations to authorized personnel and access rights be reviewed, updated and/or revoked as and when necessary; and

10.3.8 Installation, disconnection, modification or relocation of ICT resources shall only be performed with authority of Head of ICT.

11.0 INCIDENT MANAGEMENT POLICY

Incident management is the process of describing the activities that enable organizations to identify, analyze, correct and prevent a future re-occurrence of security incidents.

11.1 SCOPE

The scope covers incidents that come up from cyber-attacks as well as natural disasters.

11.2 POLICY STATEMENT

The development, implementation and execution of a Security Incident Response Plan (SIRP) shall be the primary responsibility of the specific MCDA for whom the SIRP is being developed in cooperation with the ICT InfoSec team and in reference to stipulated GoK ICT standards and procedures.

11.3 GUIDELINES

11.3.1 The SIRP shall include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. The SIRP document must include all phone numbers and email addresses for the dedicated team member(s).

11.3.2 The SIRP shall define triage steps to be coordinated with the security incident management team with the goal of swift security vulnerability mitigation.

11.3.3 The SIRP shall include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

11.3.4 The SIRP shall include levels of response to identified incidents that define the expected timelines for repair based on severity and impact to the information system.

ANNEXES

ANNEX A: ICT SECURITY ROLES

1. Executive Management

- Ensure that an appropriate risk-based Information Security Program is implemented to protect the confidentiality, integrity, and availability of all **Information Resources** collected or maintained by or on behalf of (District/Organization).
- Ensure that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.
- Ensure adequate information security financial and personnel resources are included in the budgeting and/or financial planning process.
- Ensure that the Security Team is given the necessary authority to secure the **Information Resources** under their control within the scope of the (District/Organization) Information Security Program.
- Designate an Information Security Officer and delegate authority to that individual to ensure compliance with applicable information security requirements.
- Ensure that the Information Security Officer, in coordination with the Security Team, reports annually to Executive Management on the effectiveness of the (District/Organization) Information Security Program.

2. Chief Information Security Officer (CISO)

- Oversee the entire information security program
- Develop the overall security strategy
- Communicate why security matters to the executive team
- Align business goals with security
- Oversee compliance requirements
- Plan for business continuity
- Develop a plan for loss prevention and fraud prevention
- Budget and forecast for security spend
- Define security team roles
- Handle privacy concerns

3. Data Protection Officers

- Oversee corporate data protection
- Provides guidance on data protection compliance
- Supervising data processes
- Reporting to the management on the potential threats to data security
- Auditing the data processes to assess their performance and address possible problems proactively
- Communicating with Data Protection supervisors and being a connecting link between the organization and authorities.

4. Network Security engineers (NOC)

- Configuring network security settings
- Performing penetration testing
- System administration
- Developing and implementing sufficient measures to detect cyber threats
- Implementing network security policies
- Installing and maintaining security software like firewalls or backups

5. Security Architect (SOC)/ Security Engineer

- Assessing the system's security controls and processes to find potential security gaps
- Planning changes and upgrades for corporate IT infrastructure
- Maintaining system integrity
- Implementing insider threat control measures
- Choosing new security software if needed
- Implementing disaster recovery measures
- Analyzing previous incidents and creating an incident response plan
- Analyzing the costs and benefits of security solutions

6. Application Security engineers (SOC) – subsection of security engineers.

- Configuring technical security controls
- Conducting an app risk assessment
- Whitelisting/blacklisting apps
- Performing penetration testing

7. Security Analysts (SOC) – may also be merged with incident responders/ handlers

- Analyzing and configuring corporate systems to improve their security
- Analyzing data loss prevention measures
- Looking for system vulnerabilities and ways to fix them
- Monitoring data behavior for abnormal activities
- Ethical Hacking skills
- Patch management
- Testing company's systems to locate potential risks and vulnerabilities
- Verifying security, availability, and confidentiality of corporate data

8. Incident responders (Tier 1, 2, 3) (NOC/SOC)

- Configure and manage security monitoring tools
- Malware analysis
- Execute strategies for containment, remediation and recovery
- Determine security incidences and their severity
- Monitoring data behavior for abnormal activities

9. IT Security Administrators (SOC)

- Managing access
- Ensuring that data migration is secure
- Configuring security software
- Implementing security policies
- Using software tools to automate some of the tasks

10. Information Security Auditors

- Providing independent assurance to management on the appropriateness of the security objectives
- Determining whether the security policy, standards, baselines, procedures, and guidelines are appropriate and effective to comply with the organization's security objectives
- Identifying whether the objectives and controls are being achieved

11. IT Risk Manager

- Anticipate risks the organization may be subjected to and create an action plan to minimize the negative impact
- Prepare procedures and protocols (Playbooks) for security breaches, cyber-attacks, and system failures
- Monitor technology throughout the organization for potential risks
- Attend meetings with senior leadership and providing IT perspective on business decisions
- Learning about new technologies and software that could be beneficial to the organization

ANNEX B: MCDA INFORMATION SECURITY STEERING COMMITTEE

The information security steering committee reports to Accounting Officer.

Membership:

S/No	Members	Roles
1.	Accounting officer or equivalent	Chairperson
2.	Head of ICT Unit	Member
3.	Administration Representative	Member
4.	Finance Representative(s)	Member
5.	Procurement Department Representative	Member
6.	HR Representative	Member
7.	Legal Representative	Member
8.	ICT Officers in the following areas: • InfoSec governance • Networks • Cybersecurity • System designs and development • Database administration • Data Science • Web administration • Email administration • Data center administration • Information Systems Audit • Any other member deemed necessary by the accounting officer	Members

RESPONSIBILITIES

The Committee is responsible for the following, including but not limited to:

- Assessing inventory of high-risk information assets (paper and electronic) and supporting plans to address information security weaknesses.
- Reviewing information security policies and standards and recommending improvements and revisions, as appropriate.
- Reviewing specific information security breaches and the related breach notification process.
- Serving as a liaison for the campus information security issues and help to make information security more visible within the university.
- Evaluating information security training needs.