



REPUBLIC OF KENYA
THE NATIONAL TREASURY AND ECONOMIC PLANNING



**INFORMATION SECURITY POLICY FOR PUBLIC
INVESTMENT MANAGEMENT INFORMATION SYSTEM**

May 2024

TABLE OF CONTENTS

ABBREVIATION AND ACRONYM	iv
BACKGROUND	1
VISION	2
MISSION	2
PURPOSE OF THE POLICY	2
OBJECTIVES OF THE POLICY	2
OVERALL SCOPE	4
NORMATIVE REFERENCES	4
APPLICATION OF THE POLICY	4
ENFORCEMENT	4
POLICY THEMATIC AREAS	6
1. INFORMATION SECURITY GOVERNANCE	7
1.1 MCDA GOVERNANCE STRUCTURE	7
1.2 POLICY STATEMENT.....	7
1.3 GUIDELINES.....	7
2. CYBER SECURITY MANAGEMENT	9
2.1 TELEWORKING	9
2.2 MOBILE DEVICE MANAGEMENT	10
2.3 MALWARE MANAGEMENT.....	10
2.4 BRING YOUR OWN DEVICE (BYOD)	11
3. SYSTEMS AND APPLICATIONS SECURITY	13
3.3 VIRTUALIZATION.....	16
4. COMMUNICATION SECURITY	17
4.1 NETWORK SECURITY	17
4.2 WIRELESS SECURITY.....	18
4.3 ELECTRONIC MESSAGING	19
4.4 INFORMATION SHARING	20
4.5 AGREEMENTS ON INFORMATION TRANSFER.....	21
5.INFORMATION SECURITY RISK MANAGEMENT	22

5.2 INFORMATION ASSET MANAGEMENT	23
5.3 INFORMATION CLASSIFICATION AND SHARING	24
5.4 ACCEPTABLE USE POLICY.....	25
6. HUMAN RESOURCES SECURITY	32
6.1 INTRODUCTION	32
6.2 BACKGROUND SCREENING.....	33
6.3 IN-SERVICE.....	34
6.4 TERMINATION OR CHANGE OF RESPONSIBILITIES	34
6.5 INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING.....	34
7. OPERATIONAL SECURITY.....	35
7.1 ACCESS CONTROL.....	35
7.2 CLOUD SECURITY	35
7.3 CHANGE MANAGEMENT.....	37
7.5 USER ACCOUNT MANAGEMENT	37
7.6 PASSWORD POLICY.....	38
8. PHYSICAL AND ENVIRONMENTAL SECURITY	40
8.1 SCOPE	40
8.2 POLICY STATEMENT.....	40
8.3 GUIDELINES	40
9. INCIDENT MANAGEMENT POLICY	41
9.1 SCOPE	41
9.2 POLICY STATEMENT.....	41
9.3 GUIDELINES	41
ANNEXES	41

ABBREVIATION AND ACRONYM

APIs	Application Programming Interfaces
BCP	Business Continuity Plans
BYOD	Bring Your Own Device
DRP	Disaster Recovery PLanning
GoK	Government of Kenya
GPS	Global Positioning System
ICT	Information and Communications Technology
IDS	Intrusion Detection Systems
IP	Internet Protocol
MCDAs	Ministries, Counties, Departments and Agencies
PII	Personal Identifiable Information
PIM	Public Investment Management
PIMIS	Public Investment Management Information System
VPN	Virtual Private Network
WAFs	Web application firewalls

BACKGROUND

The Government of Kenya implements a wide range of publicly funded projects and these have grown significantly, especially after the Country's constitutional change in 2010, when public investments widened with the operationalization of the 47 county governments. While public investment at the national and county levels has recorded significant socio-economic impact, they have faced various challenges, including failure to conduct rigorous project appraisals and inadequate approach to public investment management processes. For this reason, the National Treasury formulated a Public Investment Management (PIM) Framework.

The framework was issued as PIM Guidelines vide Treasury Circular No.16/2019 and later published under Legal Notice 54. of 2022 as the Public Finance (Public Investment) Management Regulations of 2022. The regulation established the Public Investment Management (PIM) department. The mandate of the Department includes:

1. Developing and maintaining a framework for project planning, conceptual design, and implementation;
2. Reviewing project concept notes for medium, large, and mega projects and recommending whether or not pre-feasibility and feasibility studies should be undertaken;
3. Reviewing pre-feasibility and feasibility studies and recommending the projects for inclusion in the project pipeline;
4. Monitoring the use of the Public Investment Management Information System;
5. Consolidating portfolio of public investment projects in the pipeline, which have been approved by accounting officers;
6. Approving new projects prioritized by accounting officers for funding where there is fiscal space;
7. Reporting on all ongoing projects that do not receive funding in the succeeding year to Cabinet and the National Assembly when submitting budget estimates;
8. Preparing analytical reports based on project data in the Public Investment Management Information System to inform decision making on policy planning and budget execution;
9. Sharing project analytical reports during the Intergovernmental Budget and Economic Council for coordination; and
10. Organizing annual public investment forums for knowledge sharing

Regulation 29 of the Public Finance Management (PIM) Regulations, 2022 establishes a Public Investment Management Information System (PIMIS) to automate the PIM process for efficient and effective investment management. The System can be accessed at <https://pimis.treasury.go.ke> for the production instance and <https://pimisdev.treasury.go.ke> for the training instance. In addition to the Project Management Cycle until pipelining, the

system has further been integrated with Kenya Revenue Authority tax management systems for a smooth tax management process of projects during the implementation phase. This has been done through a tax - exemption module in the PIMIS that will ensure that all project tax exemptions are processed through the PIMIS before submission to the Cabinet Secretary or County Executive committee for approval.

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 attacks.

VISION

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

MISSION

To secure information and information assets of the PIM system, 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 PIM Systems so as to minimize damage and reduce risk across the organization.

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. Maintain the reputation of the organization, and uphold ethical and legal responsibilities;
2. Establish a general/ overall approach to information security;
3. Detect and foretell/predict /preempt the compromise/breaches of information security such as misuse of data, networks, computer systems and applications;
4. Observe the rights of users; and
5. Provide effective mechanisms for responding to complaints and queries concerning real or perceived non-compliances with the policy.

OBJECTIVES OF THE POLICY

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

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

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

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

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).

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 PIM Information system information assets through safeguarding its confidentiality, integrity and availability;
- ii. Establish effective information security governance structure including accountability and responsibility for PIM Information system;
- 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 PIM operational environment;
- v. Ensure compliance to the relevant legal and regulatory frameworks governing PIM Information System; 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 with the GoK information security Standards, policies, guidelines, and procedures.

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.

NORMATIVE REFERENCES

This Policy is not the only document that MCDAs should look at 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 PIMIS 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; Kenya Information And Communications Act Chapter 411a (Rev 2012); Gov ICT Standards (Information Security Standard) ICTA-3.003:2023

APPLICATION OF THE POLICY

This policy applies to Government institutions using PIM Information system, and external stakeholders working within the PIMIS 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.

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.

CHALLENGES OF INFORMATION SECURITY

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.
2. Unauthorized access which may result in breach of confidentiality, alteration or loss of information.
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;
4. Malware;
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.
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.
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.
8. System Fraud: This is deliberate manipulation or modification of data and/or records for financial or personal gain.
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.
10. The spread of untrue or misleading information over electronic media especially social media is on the increase.

11. Lack of security awareness by users is a major challenge in safeguarding information security.
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, the spread of malicious applications through handheld and mobile devices is on the increase.
13. The level of cyber incident reporting in the country is very low and vague.
14. Procedures used are often counter-intuitive.
15. Requires constant monitoring.
16. Security is too often an after-thought in the onset of system design, development and roll-out.

POLICY THEMATIC AREAS

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

1. Information Security Governance
2. Cybersecurity Management
3. Systems and Applications Security
4. Communication Security
5. Information Security Risk Management
6. Human Resources Security
7. Operational Security
8. Physical and Environmental Security
9. Incident Response Management

1. 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 PIM Information system 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.

1.1 MCDA GOVERNANCE STRUCTURE

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

1.2 POLICY STATEMENT

MCDAs shall establish structures to implement information security to manage PIMIS. The accounting officer shall appoint an information security steering committee which shall ensure implementation of the information security policy, assign security roles and co-ordinate and review the implementation of security within MCDAs managing PIMIS.

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.

1.3 GUIDELINES

- 1.3.1.** 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;
- 1.3.2.** MCDAs shall implement this information security policy and provide the resources needed for its implementation;
- 1.3.3.** MCDAs shall identify the needs for internal or external specialist information security advice, and review and coordinate results of the advice.;
- 1.3.4.** The information security coordination shall involve the cooperation and collaboration of officers within government institutions implementing PIM Information System.
- 1.3.5.** MCDAs should clearly define and allocate information security responsibilities in accordance to this information security policy;

- 1.3.6.** MCDAs should clearly define and allocate information security responsibilities in accordance to this information security policy;
- 1.3.7.** Officers with allocated security responsibilities may delegate tasks to others;
- 1.3.8.** The National Treasury shall be responsible for reviewing this policy at planned intervals, or when significant changes to the security implementation occur.

DRAFT

2. 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.

2.1 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 PIM Information System users to work remotely in an authorized and secure manner while ensuring administrative efficiencies and supporting continuity of operation plans.

2.1.1 SCOPE

The stipulated guidelines shall cover both internal and external users of PIM information system.

2.1.2 POLICY STATEMENT

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

2.1.3 GUIDELINES

- 2.1.3.1** MCDAs shall be responsible for clearly communicating expectations of work assignments, check-ins, and any other parameters for supporting a remote arrangement;
- 2.1.3.2** System users shall be responsible for ensuring that they operate in an environment that is secure and conducive for teleworking;
- 2.1.3.3** MCDAs shall ensure that users are sensitized and educated on the possibilities of risks associated with teleworking;
- 2.1.3.4** MCDAs shall identify, authenticate and authorize teleworkers before giving them access to PIM information system resources;
- 2.1.3.5** Where sensitive or confidential information is being stored or accessed from off-premise, an approved access solution, such as via VPN, should be used;
- 2.1.3.6** Any loss or theft of equipment or personal equipment, which has been used to access sensitive PIM information while teleworking, shall be reported to the relevant authorities;
- 2.1.3.7** MCDAs should deploy secured equipment and/or software to ensure security is upheld in a teleworking environment.

2.2 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 PIM Information System 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.

2.2.1 SCOPE

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

2.2.2 GUIDELINES

- 2.2.2.1** The data stored in mobile devices shall be backed up frequently and measures provided for recovery;
- 2.2.2.2** 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;
- 2.2.2.3** Mobile devices accessing PIM Information System shall have the device management applications, software GPS capabilities enabled to allow location transparency and information security;
- 2.2.2.4** 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;
- 2.2.2.5** 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;
- 2.2.2.6** Mobile computing devices should have time-out protection applied, which automatically lock the device after a defined period of inactivity;
- 2.2.2.7** Mobile devices should have up-to-date genuine firmware, operating systems, anti-malware software and applications installed;
- 2.2.2.8** Officers shall not permit unauthorized users including family or friends, to use or modify any mobile device provided by the MCDA;
- 2.2.2.9** Officers who opt to use mobile computing devices not owned by the MCDA to store or access PIM Information System are fully responsible for ensuring that the device features have adequate security provisions in order to protect the information;

2.3 MALWARE MANAGEMENT

Attacks on IT Resources by malicious software have 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 PIMIS is 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.

2.3.1 SCOPE

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

2.3.2 POLICY STATEMENT

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

2.3.3 GUIDELINES

The MCDAs shall;

- 2.3.3.1** Install devices accessing PIMIS with licensed antimalware solutions such as antivirus, firewalls, intrusion, detection and prevention systems;
- 2.3.3.2** Ensure that the anti-malware software are regularly updated;
- 2.3.3.3** Restrict user access to unauthorized sources such as insecure websites and programs through firewalls and related tools;
- 2.3.3.4** Prevent users from uninstalling or disabling antimalware agents or applications in computing devices by limiting user rights;
- 2.3.3.5** Isolate suspected or infected computing devices until the threat is eliminated;
- 2.3.3.6** Ensure devices running PIM Information system are configured to automatically conduct anti-malware scan of removable media when inserted or connected;
- 2.3.3.7** Ensure devices running PIM Information system are configured not to auto-run content from removable media or online sites;
- 2.3.3.8** Do regular backups of information and information assets of PIM Information system; and
- 2.3.3.9** Regularly conduct user awareness on best security practices while using PIM Information system.

2.4 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 PIMIS and resources.

2.4.1 SCOPE

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

2.4.2 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.

2.4.3 GUIDELINES

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

MCDAs shall;

2.4.3.1 Log and monitor all personal devices accessing their PIM Information System;

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

2.4.3.3 Enforce signing of an acceptance use agreement to all PIM 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 PIM Information System
- 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.

3. SYSTEMS AND APPLICATIONS SECURITY

3.1 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 PIM Information System and applications. The purpose of this policy is to provide guidance on secure systems acquisition, development, commissioning, maintenance and decommissioning of PIM Information System in-line with the business needs and relevant procurement laws and regulations.

3.1.1 SCOPE

This policy covers the acquisition, development, commissioning, maintenance and decommissioning of all PIM Information System.

3.1.2 POLICY STATEMENT

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

3.1.3 GUIDELINES

3.1.3.1 Acquisition of systems shall conform to GoK ICT standards;

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

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

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

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

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

3.1.3.7 Appropriate change control processes for PIM Information System shall be put in place throughout the development lifecycle, coupled with technical reviews of applications for any changes made after operating platform changes;

3.1.3.8 Changes to PIM Information System shall be controlled and documented;

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

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

- 3.1.3.11** System acceptance testing and quality assurance shall be carried out for new systems, upgrades, and newer versions; and
- 3.1.3.12** The development team shall incorporate technical staff with necessary capability for avoiding, finding, and fixing vulnerabilities.

3.1.4 MAINTENANCE OF PIM INFORMATION SYSTEM

- 3.1.4.1** All applications shall be patched and updated regularly to ensure optimal and secure performance;
- 3.1.4.2** All equipment shall be maintained (preventive and corrective) regularly to ensure optimal and secure performance;
- 3.1.4.3** All active applications within PIM Information System environment shall be monitored using appropriate tools;
- 3.1.4.4** MCDAs shall maintain separate environments for production and non-production/testing of PIM Information System; and
- 3.1.4.5** MCDAs shall ensure regular backup of PIM Information System as per the provided standards, guidelines and procedures.

3.1.5 DECOMMISSIONING OF PIM INFORMATION SYSTEM

- 3.1.5.1** MCDAs shall define acceptable guidelines for identifying systems for decommissioning, in compliance with laid down Government disposal procedures;
- 3.1.5.2** 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;
- 3.1.5.3** 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 system configurations (switches, firewalls etc.)
- m. Equipment and media sanitization including any cloud based data & services
- n. Any legal considerations for supply or service contract terminations
- o. Asset register updates
- p. Retraining or redeployment of support staff.

3.2 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 a need to guide secure and effective integration of Public Financial Management Information Systems with other systems.

3.2.1 SCOPE

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

3.2.2 POLICY STATEMENT

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

3.2.3 GUIDELINES

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

- 3.2.3.1** Data formats are in accordance with the targeted systems in order to avoid transmission errors;
- 3.2.3.2** Request parameters of relevant error messaging are validated to defend against injection attacks;
- 3.2.3.3** Proper authentication and authorization is enforced to ensure that data is from authorized parties only;

- 3.2.3.4** 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;
- 3.2.3.5** Digital signatures are used to safeguard against nonrepudiation of transactions;
- 3.2.3.6** Data is encrypted using the latest technology when on transit and at rest; and
- 3.2.3.7** All PIM Information System are developed and integrated as per the Government ICT Standards on information security

3.3 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.

3.3.1 SCOPE

This covers PIM Information System deployed and operating in virtualized environments.

3.3.2 POLICY STATEMENT

To evaluate, monitor and manage security within a virtual environment in PIM Information System.

3.3.3 GUIDELINES

In the deployment of virtualization technology MCDAs shall:

- 3.3.3.1** Ensure the security of each virtual machine;
- 3.3.3.2** Secure virtual networks from attacks and vulnerabilities that may surface from the underlying physical environment;
- 3.3.3.3** Ensure guest operating system is isolated from the host operating system;
- 3.3.3.4** Ensure both the host and virtual environment are only accessed by authorized user(s);
- 3.3.3.5** Ensure virtualization software is up-to-date with vendor patch releases;
- 3.3.3.6** Ensure access and visibility between the guests hosted within the host operating systems shall be restricted; and
- 3.3.3.7** Routinely inspect and monitor the virtualization environment, perform audits to flag suspicious configurations and communication between the guests.

4. COMMUNICATION SECURITY

This stipulates how the PIM Information System 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 PIM 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.

4.1 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 an integral part in communication and sharing of resources, data and applications. Network Security guides on use, protection and security of information in networks for PIM Information System.

4.1.1 SCOPE

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

4.1.2 POLICY STATEMENT

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

4.1.3 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;

- 4.1.3.1** Ensure network operations related passwords e.g. for switches and routers are securely stored;
- 4.1.3.2** Ensure regular scans are performed from outside each trusted network perimeter to detect any unauthorized connections which are accessible across the boundary;
- 4.1.3.3** 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;

- 4.1.3.4** 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;
- 4.1.3.5** 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;
- 4.1.3.6** Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries;
- 4.1.3.7** Enable the collection and monitoring of network flows and logging data on network boundary devices;
- 4.1.3.8** Ensure that all network traffic to or from the Internet passes
- 4.1.3.9** through an authenticated application layer proxy that is configured to filter unauthorized connections;
- 4.1.3.10** Require all remote login access to their network is encrypted;
- 4.1.3.11** Maintain standard, documented security configurations for all authorized network devices;
- 4.1.3.12** Compare all network device configurations against approved security configurations defined for each network device in use and alert when any deviations are discovered;
- 4.1.3.13** Install the latest stable version of any security related updates on all network devices;
- 4.1.3.14** Manage network devices using multi-factor authentication and encrypted sessions where possible;
- 4.1.3.15** Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system;
- 4.1.3.16** 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;
- 4.1.3.17** 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;
- 4.1.3.18** Automatically disconnect users connected through a VPN after prescribed time of inactivity;

4.2 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 PIM Information System networks.

4.2.1 SCOPE

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

4.2.2 POLICY STATEMENT

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

4.2.3 GUIDELINES

MCDAs shall:

- 4.2.3.1** 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;
- 4.2.3.2** Maintain an inventory of authorized wireless access points connected to the wired network;
- 4.2.3.3** Configure network vulnerability scanning tools to monitor, detect and alert on unauthorized wireless access points connected to the wired network;
- 4.2.3.4** 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;
- 4.2.3.5** Leverage on wireless encryption standards for data in transit;
- 4.2.3.6** Ensure that wireless networks use authentication protocols; and **6.2.3.7** Scan wireless devices for malware before admission to the network.

4.3 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 PIM Information System.

4.3.1 SCOPE

Electronic Messaging covers all aspects of electronic messaging as used in the PIM Information System.

4.3.2 POLICY STATEMENT

Security controls shall be established to protect electronic messaging from unauthorized access, modifications or denial of service. Electronic messages on PIM Information System are considered organization's information assets and as such, the PIM

Information System owners shall have the right to access, control and examine such messages on a need basis.

4.3.3 GUIDELINES

- 4.3.3.1** 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;
- 4.3.3.2** Protected and/or confidential information shall not be entered in the subject line of any electronic message.
- 4.3.3.3** PIM Information System users shall not provide their login ID or password to another person or vendor due to potential security risks;
- 4.3.3.4** Auto-forwarding emails containing protected information to any external mail service shall not be permitted;
- 4.3.3.5** PIM Information System users shall not subject their official email accounts for private communication;
- 4.3.3.6** MCDAs shall install anti-malware software that shall auto-scan attachments before they are opened by users;
- 4.3.3.7** When dealing with external stakeholders for official communication,
 - a.** PIM Information System users shall only use official emails
 - b.** Avoid confidential information in subject line;
- 4.3.3.8** All PIM Information System users shall employ electronic messaging practices in accordance with GoK ICT Security Standard.

4.4 INFORMATION SHARING

PIM Information System place a strong emphasis on the need to share information across organizational and professional boundaries, in order to ensure effective coordination and integration of services. This calls for the embedding of security and confidentiality in relation to all information held by PIM Information System 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 PIM Information System providing data to a third party or parties;
- c.** Several PIM Information System 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.

4.4.1 SCOPE

This covers all aspects of information sharing in PIM Information System while ensuring security of the information.

4.4.2 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.

4.4.3 GUIDELINES

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

4.4.3.2 The PIM Information System Users shall adhere to controls and restrictions associated with using communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses;

4.4.3.3 The PIM Information System Users shall take appropriate precautions not to reveal confidential information; and

4.4.3.4 PIM Information System owners shall develop procedures to safeguard transfer of information in accordance with GoK ICT Security Standard.

4.5 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 PIM Information System.

4.5.1 SCOPE

This covers all agreements on information transfer as executed in the PIM Information System.

4.5.2 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.

4.5.3 GUIDELINES

4.5.3.1 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;

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

4.5.3.3 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.

5. INFORMATION SECURITY RISK MANAGEMENT

Risk management is the process of identifying vulnerabilities and threats to the information resources used by PIM Information System 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.

5.1.1 SCOPE

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

5.1.2 POLICY STATEMENT

The MCDAs operating PIM Information System 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.

5.1.3 GUIDELINES

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

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

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

5.2 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 PIM Information System.

Information assets include;

- a. operating systems
- b. infrastructure
- c. applications
- d. records
- e. Data and information
- f. ICT hardware

5.2.1 SCOPE

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

5.2.2 POLICY STATEMENT

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

5.2.3 GUIDELINES

5.2.3.1 An inventory of all information assets shall be implemented and maintained for PIM Information System;

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

- 5.2.3.3** Information assets shall be maintained regularly as per the manufacturers' recommendations;
- 5.2.3.4** Proper security of information assets shall be maintained when the asset is decommissioned, disposed or destroyed;
- 5.2.3.5** Information system owners shall define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies;
- 5.2.3.6** Rules for the acceptable use of information and associated assets with information and information processing facilities shall be identified, implemented and documented;
- 5.2.3.7** Officers and external users shall return all MCDAs information assets in their possession upon termination of their employment, contract or agreement;
- 5.2.3.8** 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;
- 5.2.3.9** 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;
- 5.2.3.10** The MCDAs shall control copying of sensitive information;
- 5.2.3.11** MCDAs shall implement appropriate controls when the information asset is scheduled for maintenance;
- 5.2.3.12** Before putting the information asset back into operation after maintenance, it shall be inspected to ensure that it has not been tampered with;
- 5.2.3.13** Formal procedures shall be documented for secure disposal of media and assets to minimize the risk of confidential information leakage to unauthorized persons;
- 5.2.3.14** 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
- 5.2.3.15** MCDAs shall ensure storage of ICT assets in accordance with manufacturers' specifications.

5.3 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.

5.3.1 SCOPE

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

5.3.2 POLICY STATEMENT

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

5.3.3 GUIDELINES

- 5.3.3.1** MCDAs shall classify information as per the scheme above. It shall classify; information stored in physical form, electronic form and communications medium;
- 5.3.3.2** Information shall be classified in line of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification;
- 5.3.3.3** MCDAs shall ensure protection of temporary or permanent copies of information to a level consistent with the protection of the original information;
- 5.3.3.4** MCDAs shall ensure clear marking of all copies of media for the attention of the authorized recipient;
- 5.3.3.5** 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.

5.4 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 PIM 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.

5.4.1 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.

5.4.2 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.

5.4.3 GUIDELINES

- 5.4.3.1** 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.
- 5.4.3.2** 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.
- 5.4.3.3** Use of ICT resources must comply with applicable laws.
- 5.4.3.4** Use of ICT resources shall be monitored to check adherence to this security policy, standards and guidelines.
- 5.4.3.5** Visiting sites that contain illegal material or in violation of MCDAs policies or local laws is prohibited;
- 5.4.3.6** Using the Internet to send offensive or harassing material to other people is prohibited;
- 5.4.3.7** Employees shall not be allowed to perpetrate any form of fraud or illegal activities;
- 5.4.3.8** 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;

- 5.4.3.9** Performing any form of hacking including but not limited to reconnaissance, scanning, and trying to gain unauthorized access into MCDAs information assets is prohibited;
- 5.4.3.10** Intentionally introducing malicious code, including, but not limited to viruses, worms, Trojan horses, e-mail bombs, spyware, adware and key loggers is prohibited.
- 5.4.3.11** 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.
- 5.4.3.12** Unauthorized changing of the configuration settings or naming standards of the information assets is prohibited.
- 5.4.3.13** Spamming is prohibited.
- 5.4.3.14** Forging, misrepresenting, obscuring, suppressing or replacing a user identity on any electronic communication to mislead the recipient about the sender is prohibited.
- 5.4.3.15** Revealing confidential information about MCDAs in a personal online posting, upload or transmission is prohibited;
- 5.4.3.16** 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.
- 5.4.3.17** Using any of MCDAs ICT facilities for personal commercial gain (including advertising) is prohibited;

5.5 BUSINESS CONTINUITY MANAGEMENT

Business Continuity Management provides a framework for advanced planning and preparation of MCDAs to maintain PIM Information System 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.

5.5.1 SCOPE

It covers all the PIM Information System resources and personnel that support critical business processes.

5.5.2 POLICY STATEMENT

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

5.5.3 GUIDELINES

5.5.3.1 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

5.5.3.2 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 and updated on an annual basis.

5.5.3.3 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
 - Accurate and complete records of the backup copies and documented restoration procedures;
 - The extent (e.g. full or differential backup) and frequency of backups;
 - Criticality of the information for the continuity of operations of the organization;
- iii. The backups shall be stored in a remote location, at a sufficient physical distance.
- iv. Backup information shall be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site;

- v. 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;
- vi. 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;
- vii. In situations where confidentiality is of importance, backups shall be protected by means of encryption;
- viii. Operational procedures shall monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups;
- ix. Backup arrangements for individual systems and services shall be regularly tested to ensure that they meet the requirements of business continuity plans.
- x. The retention period for essential business information shall be determined, taking into account any requirement for archive copies to be permanently retained.

5.6.1 SCOPE

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

5.6.2 POLICY STATEMENT

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

5.6.3 GUIDELINES

- 5.6.3.1** 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;
- 5.6.3.2** Timelines shall be defined to react to notifications of potentially relevant vulnerabilities;
- 5.6.3.3** Procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks shall be developed;
- 5.6.3.4** 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;
- 5.6.3.5** 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;
- 5.6.3.6** MCDAs shall carry out installation and regular updates of antimalware software;

- 5.6.3.7** MCDAs shall define a procedure to address the situation where vulnerability has been identified but there is no suitable countermeasure;
- 5.6.3.8** 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 to the 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.
- 5.6.3.9** 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;
- 5.6.3.10** Use of unauthorized software is prohibited and MCDAs should implement controls that prevent or detect the use of unauthorized software and suspected malicious websites.

6. HUMAN RESOURCES SECURITY

6.1 INTRODUCTION

This is to provide Public Investment Management Information System 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;

6.1.1 SCOPE

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

6.1.2 POLICY STATEMENT

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

6.1.3 GUIDELINES

MCDAs shall manage human resource security in the following ways:

- 6.1.3.1** Provide management direction and support for information security in accordance with business requirements, this policy and other relevant laws and regulations;
- 6.1.3.2** Responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the officer and enforced;
- 6.1.3.3** New system users shall be trained on system use;
- 6.1.3.4** Ensure that all stakeholders are aware of and fulfill their information security responsibilities and by signing a non-disclosure agreement
- 6.1.3.5** Protect the MCDAs interests as part of the process of changing or terminating employment.
- 6.1.3.6** 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.

6.2 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.

6.2.1 POLICY STATEMENT

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

6.2.2 GUIDELINES

- 6.2.2.1** MCDAs shall conduct background verification checks on all candidates for employment in accordance with relevant laws, regulations and ethics;
- 6.2.2.2** The screening shall be proportional to the MCDAs requirements, the classification of the information to be accessed and the perceived risks;
- 6.2.2.3** Internal promotions that involves the person accessing mission critical assets shall also attract further and more detailed vetting.

6.3 IN-SERVICE

6.3.1 POLICY STATEMENT

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

6.3.2 GUIDELINES

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

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

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

6.4 TERMINATION OR CHANGE OF RESPONSIBILITIES

6.4.1 POLICY STATEMENT

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

6.4.2 GUIDELINES

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

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

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

6.5 INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

6.5.1 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.

6.5.2 GUIDELINES

6.5.2.1 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;

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

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

7. OPERATIONAL SECURITY

Security of PIM Information System 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.

7.1 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 PIM Information System resulting from unauthorized use of resources.

7.1.1 POLICY STATEMENT

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

7.1.2 GUIDELINES

- 7.1.2.1 Access rights and privileges to PIM Information System shall be assigned based on user's roles and responsibilities on the respective systems and applications;
- 7.1.2.2 User access passwords shall conform to the section on passwords in this policy (Clause 9.5);
- 7.1.2.3 All PIM Information System shall have audit logs to track users' activity and be monitored regularly;
- 7.1.2.4 Remote access to the PIM Information System shall be allowed through an authorized secure connection e.g. VPN;
- 7.1.2.5 Periodic audits of access controls and user rights shall be conducted to ensure they are working as expected;
- 7.1.2.6 MCDAs shall ensure periodical identification, disabling and retire inactive user IDs;
- 7.1.2.7 Access to program source codes shall be restricted to authorized personnel and shall be written in English language.

7.2 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 PIM Information System.

7.2.1 SCOPE

This policy covers the acquisition and deployment of cloud based PIM Information System.

7.2.2 POLICY STATEMENT

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

7.2.3 GUIDELINES

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

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

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

7.2.3.3 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.

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

7.3 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 PIM Information System operational environment in order to ensure that they are carried out in a planned manner to minimize negative impact to services.

7.4.1 SCOPE

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

7.4.2 POLICY STATEMENT

Changes to configurations, systems, applications or equipment that affect PIM Information System 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.

7.4.3 GUIDELINES

- 7.4.3.1** MCDAs shall ensure identification and recording of significant changes that affect PIM Information System;
- 7.4.3.2** All changes shall be planned, tested and communicated to all relevant stakeholders;
- 7.4.3.3** MCDAs shall ensure that assessment of the potential impacts, including information security impacts of changes in PIM Information System are documented;
- 7.4.3.4** Changes requested by users shall contain sufficient information to enable the evaluation of the potential risks and benefits;
- 7.4.3.5** A roll-back plan shall be developed and tested before a change is implemented;
- 7.4.3.6** MCDAs shall ensure changes are effected without disrupting service delivery;
- 7.4.3.7** Users shall be notified of the changes made on the PIM Information System and taken through training on the new operational processes impacted by a change in PIM Information System.
- 7.4.3.8** Users shall review and accept completion of the changes in readiness for transition to production environment and the review shall be documented;
- 7.4.3.9** An audit log of all relevant information on the changes shall be retained.

7.5 USER ACCOUNT MANAGEMENT

There is need to carefully manage all user accounts, especially those accounts that have administrative rights on the PIM Information System. 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.

7.5.1 SCOPE

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

7.5.2 POLICY STATEMENT

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

7.5.3 GUIDELINES

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

7.5.3.2 All user accounts must be uniquely created and identifiable;

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

7.5.3.4 Users shall be granted privileges that are commensurate with their roles and responsibilities in the PIM Information System;

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

7.5.3.6 All users must refrain from abuse of privilege;

7.5.3.7 All accounts access must meet the PIM Information System Password Policy;

7.5.3.8 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;

7.5.3.9 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.

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

7.6 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 PIM Information System. The purpose of this policy is to establish guidelines for creation of strong passwords, the protection of those passwords and the frequency of change.

7.6.1 SCOPE

The policy covers all users who access the PIM Information System.

7.6.2 POLICY STATEMENT

All users accessing the PIM Information System shall be authenticated using a password.

7.6.2 GUIDELINES

- 7.6.2.1** Passwords shall be used on all PIM automated information systems to uniquely identify individual users;
- 7.6.2.2** Password complexity design shall be incorporated in all PIM Information System to include the following: have at least 6 characters, upper case, lower case, special characters and numbers;
- 7.6.2.3** Passwords shall not be shared amongst users, neither be generic;
- 7.6.2.4** 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;
- 7.6.2.5** Passwords shall expire after every 90 days;
- 7.6.2.6** Password should not be dictionary words;
- 7.6.2.7** Passwords shall not be portions of associated account names (e.g. user ID, log-in name, personal information);
- 7.6.2.8** Passwords shall not be character strings (e.g. abc or 123);
- 7.6.2.9** Passwords shall not be simple keyboard patterns (e.g. QWERTY, asdf);
- 7.6.2.10** Users are responsible for the security of their password(s) and shall be accountable for any misuse;
- 7.6.2.11** Incidents where accounts are suspected to have been compromised shall be reported to the system administrator;
- 7.6.2.12** Any default passwords must be changed on all systems prior to connection to any network including pre-deployment testing;
- 7.6.2.13** Systems should be configured to lock a session after a pre-determined time of inactivity;
- 7.6.2.14** 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 PIMIS facilities by the system administrator;

8. PHYSICAL AND ENVIRONMENTAL SECURITY

PIM Information System is 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 PIM Information System environment.

8.1 SCOPE

This policy covers all information processing facilities for PIM Information System.

8.2 POLICY STATEMENT

MCDAs shall ensure protection of critical and sensitive PIM Information System information processing facilities.

8.3 GUIDELINES

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

- 8.3.1** Removable media (flash disks, portable hard drives) should be securely stored when not in use and kept away from environmental hazards;
- 8.3.2** MCDAs shall ensure installation of clean power to protect PIMIS equipment from damage;
- 8.3.3** 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;
- 8.3.4** Employees should exercise care to safeguard the valuable electronic equipment assigned to them failure to which they shall be held accountable;
- 8.3.5** MCDAs shall ensure ICT facilities are hosted within physically and environmentally secured areas;
- 8.3.6** MCDAs shall deploy surveillance and monitoring mechanisms to cover all critical ICT equipment installations;
- 8.3.7** 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
- 8.3.8** Installation, disconnection, modification or relocation of ICT resources shall only be performed with authority of Head of ICT.

9. 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.

9.1 SCOPE

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

9.2 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.

9.3 GUIDELINES

- 9.3.1** 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).
- 9.3.2** The SIRP shall define triage steps to be coordinated with the security incident management team with the goal of swift security vulnerability mitigation.
- 9.3.3** 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.
- 9.3.4** 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

User Roles as defined in the system

1. System Super Administrator

- Management of the System Administration Centre
- Assigning access user rights to all the other system administrators in the system.
- Assigning and reassigning user rights in the system as guided by the Accounting Officer
- Producing dynamic reports for all the projects at all levels of implementation.
- Overall system user support

2. System Administrator

- Assigning and reassigning user rights in the system as guided by the Accounting Officer of the relevant MDCA. All the actors must be approved by the Accounting Officer and the appointment letter be attached to the system. The other system users created by the system administrator are: Project proposer, Project Reviewer, Project Approver, Budget proposer, Project Manager, Project Contractors
- Producing dynamic reports from the system for projects within their various MDCAs.
- User support in the system within their respective MDCAs.
- Activate, deactivate and block user with the direction and approval from the Accounting Officer

3. Project Proposer (Head of Department/Section/Unit or Equivalent)

- Creating a PCN in the system
- Editing the created PCN before submission
- Forwarding (submitting) the PCN to the project committee for review.

4. Project Reviewer (Project Committee Chair Person or/and Secretary)

The project committee shall be appointed by the accounting officer in the National Government

state department or its entities shall attach the minutes' of the committee meeting deliberations.

5. Project Approver (Accounting Officer)

The accounting officer being the head of MDCA shall ensure:

- Project conceptual designs are done using the logical framework analysis and develop
- the logical framework matrix as per the PIM regulations
- That the recommendations of the Project Committee on the PCN are considered
- before making a decision.
- Approve the PCN for a small project (with no specialized technical solutions)
- Submit PCNs for small projects (Kshs 500 million and below) with no specialized
- technical solutions to the project pipeline (bank of projects) of the Public Investment
- Management Information System.
- Submits the medium, large and mega projects (Khs 500 million and above) to the
- National Treasury for independent appraisal.
- Approves all the users assigned/reassigned rights in the system
- Receives monthly, quarterly and annual project progress reports

- Ensure that all conditions precedent are fulfilled, including land acquisition,
- compensation, stakeholder management and development partners' requirements
- have been met
- Prioritize the project in the project pipeline (bank of projects) as per the organization
- mandate and the fiscal space to onboard the new project into implementation.

6. Project Manager

- Coming up with the project implementation workplan
- Setting the activity weights
- Day to day monitoring of the project
- Updates the day to day project progress through various projects activities
- Reports on the project progress through the M&E reporting matrix in the system
- Submits monthly, quarterly and annual reports to the project reviewer (project committee)

7. Budget proposer

Update the budget estimates for the State Department and submit the same to the National Treasury budget planning system (IFMIS- Hyperion)

8. Independent project appraisal in the National Treasury workflow

Below are the responsibilities of the key players in the National Treasury Workflow.

- a. Project Appraiser (Director PIM)
- b. TNT Reviewer 1 (Director General)
- c. TNT Reviewer II (PS)
- d. TNT Approver (CS)