Information Security Policy
For
PUBLIC FINANCE MANAGEMENT (PFM) SYSTEMS

October, 2021

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 evil purposes through computer based fraud, data theft, surveillance or vandalism etc.

The Public Financial Management (PFM) systems are prone to such vulnerabilities which could impede the progress made in the use of technology in service delivery and 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 systems.

This policy therefore provides the framework for development and maintenance of PFM systems that are flexible and efficient; secure and reliable and provides confidence in digital capabilities.

Additionally, recent legislations require entities to protect personal 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 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 the people who participated in the development of the policy.

Dr. Julius Muia, PhD, CBS

Principal Secretary, National Treasury

Vision

To build secure and resilient PFM systems that promote socio-economic development.

Mission

To protect information and information assets of PFM systems, build capabilities to prevent and respond to information security threats, reduce vulnerabilities and minimize damage through a combination of institutional structures, people, processes, technology and collaboration.

Table of Contents

FOREWORD **2**

INTRODUCTION **7**

PURPOSE **8**

SCOPE **9**

APPLICATION **9**

POLICY STATEMENT **9**

General Policy Guidelines 10

INFORMATION SECURITY GOVERNANCE **11**

INTERNAL ORGANIZATION 11

Policy Statement 11

Policy guidelines 12

EXTERNAL ENTITIES 13

Scope 13

Policy Statement 13

Policy Guidelines 13

CYBER SECURITY MANAGEMENT **14**

Introduction 14

Purpose 14

TELEWORKING 14

MOBILE DEVICE MANAGEMENT POLICY 16

MALWARE MANAGEMENT 18

BRING YOUR OWN DEVICE POLICY 19

SYSTEMS AND APPLICATIONS SECURITY **21**

SYSTEMS ACQUISITION MAINTENANCE AND DECOMMISSIONING 21

APIs AND INTEROPERABILITY 24

VIRTUALIZATION 25

COMMUNICATION SECURITY **27**

NETWORK SECURITY 28

WIRELESS SECURITY 32

ELECTRONIC MESSAGING 34

INFORMATION SHARING 36

AGREEMENTS ON INFORMATION TRANSFER 38

INFORMATION SECURITY RISK MANAGEMENT **40**

INFORMATION ASSET MANAGEMENT 41
INFORMATION CLASSIFICATION AND SHARING 42
BUSINESS CONTINUITY MANAGEMENT 45
THREAT AND VULNERABILITY MANAGEMENT 46
DISASTER RECOVERY PLAN Policy 48
HUMAN RESOURCES SECURITY 50
BACKGROUND SCREENING 51
IN-SERVICE 51
TERMINATION OR CHANGE OF RESPONSIBILITIES 52
INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING 52
OPERATIONAL SECURITY 54
ACCESS CONTROL POLICY 54
Logical Access Control Policy 54
CLOUD SECURITY 55
CHANGE MANAGEMENT 56
USER ACCOUNT MANAGEMENT Policy 58
PASSWORD POLICY 60
PHYSICAL AND ENVIRONMENTAL SECURITY 63
INCIDENT RESPONSE PLAN Policy 65

Terms and Definitions

Availability	Having appropriate access to Information Assets as and when required in the course of the Institutions' operations
Confidentiality	The restriction of information to those persons who are authorized to receive or access it
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 theInstitution. . Key Information Assets are the most important types of information required for achievement of the Institutions' strategic objectives
Integrity	The completeness and preservation of information in its original and intended form unless amended or deleted by authorised people or processes.
Quality	The state of completeness, validity, consistency, timeliness and accuracy that makes data appropriate for both operational and strategic use.
Information Security Unit	Department/ Unit responsible for the function for information security within the institution.
MCDA	Ministries, Counties, Departments and Agencies
PFM System	Public Finance Management system
NDA	Non-Disclosure Agreement
InfoSec	Information Security
GPS	Global Positioning System
API	Application Programming Interface
VPN	Virtual Private Network

INTRODUCTION

The National Treasury derives its mandate from Article 225 (1) of the Constitution of Kenya, 2010, which states that an Act of Parliament shall provide for the establishment, functions and responsibilities of the National Treasury whose provision is actualized in the Public Finance Management Act (PFM) Act 2012. Further, the functions and obligations of the National Treasury and Planning are drawn from the Executive Order No.1 of 2020 (Revised). The core functions include:

- Overall Economic Policy and Public Finance Management;
- Formulation of National Budget;
- Public Debt Management;
- Formulation and Maintenance of Government Accounting Standards and Oversight Over Revenue;
- Bilateral and Multilateral Financial Relations;
- Formulation and Management of National Pensions; Market Competition and Consumer protection; Insurance; and Public Procurement and Disposal Policies;
- Public Investment Policy and Oversight;
- Development and Enforcement of Financial Governance Standards and Oversight;
- Management of National and County Governments Financial Systems and Standards;
- Development of Kenya as an International Financial Centre;
- Custodian of National Government Assets and Property;
- National and Sectoral Development Planning;
- National Statistics, Census and Housing Surveys Management;
- Population Policy Management;
- Monitoring and Evaluation of Economic Trends;
- Coordination of Implementation, Monitoring and Evaluation of Sustainable Development Goals (SDGs) and Liaison with Economic Commission for Africa; and
- Promotion of Equity through Affirmative Action Programmes and National Government Constituency Development Fund.

The Role of the National Treasury and Planning in the Devolved System of Government

The National Treasury and Planning is mandated by law to:

- Strengthen financial and fiscal relations between the National Government and County Governments and support for county governments in performing their functions;
- Issue guidelines on the preparation of county development planning;
- Prepare the annual legislative proposals on intergovernmental fiscal transfers;
- Provide logistical support to intergovernmental institutions overseeing intergovernmental fiscal relations;
- Coordinate the development and implementation of financial recovery plans for County Governments that are in financial distress;
- Build capacity of County Governments on public finance management matters for efficient, effective and transparent financial management as well as planning, monitoring and evaluation; and,
- Administer the Equalization Fund.

For most organizations government included, information, and the knowledge based on it, is one of their most important assets because conducting business without it would not be possible. The systems and processes that handle this information have become pervasive throughout organizations across the globe. This reliance on information and their related systems have made information security governance a critical facet of overall enterprise governance. In addition to addressing legal and regulatory requirements, effective information security governance plays a critical role in service delivery.

PURPOSE

This policy is designed to mitigate risk in response to actual or perceived threats. The policy states management intent and direction at a high level by demonstrating support for implementation of the information security strategy.

The specific objectives of this policy are to:

1) Protect the PFM systems information assets through safeguarding its confidentiality, integrity and availability
2) Establish effective information security governance structure including accountability and responsibility for PFM systems
3) Maintain an appropriate stakeholder awareness, knowledge and skill to minimize the occurrence and severity of information

security incidents

4) 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.
5) Ensure compliance to the relevant legal and regulatory frameworks governing PFM systems.
6) Provide the principles by which a safe and secure information systems working environment can be established for users, suppliers and third party and any other authorized users.

SCOPE

This Policy provides guidelines for the holistic management of information security risks within PFM systems operational environment including but not limited to Information Security governance, cyber security management, systems and applications security, communication security and human resource security.

APPLICATION

This policy applies to both internal and external stakeholders that interact with PFM systems operational environment and all MCDAs managing or using PFM systems.

POLICY STATEMENT

The National Treasury 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 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 levels.

The policy's goal is to protect PFM systems operational environment against all internal, external, deliberate or accidental threats.

General Policy Guidelines

The National Treasury and all MCDAs managing PFM systems shall:

1) Ensure that Information security governance is integrated into the overall enterprise governance structure hence supporting organizational goals by the information security program.
2) Deploy internal metrics and ensure continuous monitoring of changing security conditions.
3) Conduct security audits in accordance with Government regulations as well as best practice.
4) Assign responsibilities related to information security and risk management.

Enforcement

The Principal Secretary shall ensure enforcement and compliance to this policy but the overall oversight rests with the ICT Steering Committee.

Violation of any section of this policy will be treated as misconduct and the necessary disciplinary measures taken as stipulated in Public s

Service HR manual and other relevant legislations.

Exceptions

Any exception to the policy must be approved by Accounting Officer through the Head of ICT/ Infosec in advance.

INFORMATION SECURITY GOVERNANCE

Introduction

The Security Governance policy aims to ensure internal organization 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.

Purpose

The purpose of this policy is to create an information security management framework within PFM 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.

INTERNAL ORGANIZATION

Scope

This policy covers internal organization of information security in MCDAs managing PFM 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.

Policy Statement

A management framework shall be established to initiate and control the implementation of information security within MCDAs managing PFM systems.

Management shall approve the information security policy, assign security roles and co-ordinate and review the implementation of security across MCDAs managing PFM systems.

Where necessary, a source of specialist information security advice should be established and made available within the MCDA.

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.

Policy guidelines

1) Management should actively support security within the MCDA through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
2) Management shall formulate, review, approve information security policy and provide the resources needed for security implementation
3) Management should identify the needs for internal or external specialist information security advice, and review and coordinate results of the advice throughout the MCDA.
4) The information security co-ordination should involve the co-operation and collaboration of managers, users, administrators, application designers, auditors and security personnel, and specialist skills in areas such as insurance, legal issues, human resources, IT or risk management.
5) All information security responsibilities should be clearly defined and allocated in accordance with the information security policy.
6) Individuals with allocated security responsibilities may delegate security tasks to others. Nevertheless they remain responsible and should determine that any delegated tasks have been correctly performed.
7) A management authorization process for new information processing facilities should be defined and implemented.
8) Where necessary, hardware and software should be checked to ensure that they are compatible with other system components
9) The use of personal or privately owned information processing facilities, e.g. laptops, home-computers or hand-held devices, for processing business information, may introduce new vulnerabilities and necessary controls should be identified and implemented.
10) Requirements for confidentiality or non-disclosure agreements reflecting the MCDA's needs for the protection of information should be identified and regularly reviewed.
11) MCDAs should have procedures in place that specify when and by whom authorities (e.g. law enforcement, fire department, supervisory authorities) should be contacted, and how identified information security incidents should be reported in a timely manner if it is suspected that laws may have been infringed.
12) Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.
13) The MCDA's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

EXTERNAL ENTITIES

An important aspect of information security governance is the rules and processes employed when dealing with third-party relationships. These include Service providers, Outsourced operations, trading partners, merged or acquired organizations and the public.

Scope

This policy covers identification of risks related to external entities, addressing security when dealing with clients and security in third party agreements.

Policy Statement

A management framework shall be established to maintain the security of the PFM systems operational environment that are accessed, processed, communicated to, or managed by external parties.

Any access to the PFM systems operational environment by external parties should be controlled.

Where there is a business need for working with external parties that may require access to the PFM systems operational environment, or in obtaining or providing a product and service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements.

Controls shall be agreed and defined in an agreement with the external party.

Policy Guidelines

1) The risks to the PFM systems operational environment involving external parties should be identified and appropriate controls implemented before granting access.
2) Where feasible, the respective MCDA should sign a contract defining the terms and conditions for the connection or access and the working arrangement.
3) Generally, all security requirements resulting from work with external parties should be reflected by the agreement with the external party.
4) MCDAs should ensure that the external parties are aware of their obligations, and accept the responsibilities and liabilities involved in accessing, processing, communicating, or managing PFM systems operational environment.

5) All identified security requirements should be addressed in accordance with the access control policy before granting clients access to the PFM systems operational environment or assets.
6) Agreements with third parties involving accessing, processing, communicating or managing the PFM systems operational environment should cover all relevant security requirements.

CYBER SECURITY MANAGEMENT

Introduction

Cyber security management can be described as what MCDAs do to protect information systems and computer networks from cyber-attacks and threats.

Purpose

The purpose of this policy is to protect PFM systems and computer networks from cyber-attacks and threats.

TELEWORKING

Introduction

Teleworking, also known as telecommuting, means working from home or from a location outside an employer's office using modern technology and telecommunications including but not limited to computers, telephones, email and the internet.

Policy Objective

This policy provides guidelines and procedures that allow employees to work remotely in an authorized and secure manner while ensuring administrative efficiencies and supporting continuity of operation plans for PFM Systems operational environment.

Scope

This policy covers all aspects of teleworking for PFM systems operational environment.

Application

This teleworking policy shall be applicable to all PFM Systems users who undertake teleworking.

Policy Statements

The MCDA shall determine assignments eligible for teleworking subject to approval.

All Human Resource policies, procedures and agreements shall remain in effect, regardless of work locations.

Consistent with the organization's expectations of information security for employees working at the office, teleworking employees shall be expected to ensure the protection of information accessible remotely.

Policy Guidelines

1) Supervisors shall be responsible for clearly communicating expectations of work assignments, check-ins, and any other parameters for supporting a remote arrangement.
2) The employees shall be available for work as per HR Policies and procedures Manual.
3) Where office equipment is provided, the employee shall ensure compliance with acceptable use policy.
4) Employees shall only seek for technical support from on-site teams or an authorized contractor when working remotely.
5) The employee shall ensure that they create and / or use an environment that is secure and conducive for teleworking.
6) There should be prior communication on teleworking arrangement including review of the same.

Enforcement

MOBILE DEVICE MANAGEMENT POLICY

Introduction

Purpose

The aim of this policy is to provide PFM Systems users with guidelines and requirements regarding security of data, information and communications.

Devices covered, include but not limited to Laptops, Tablets, Mobile phones/Smart Phones and any other mobile IoT.

Policy objectives

This policy provides guidance to secure data and communications while using mobile devices.

Scope

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

Application

This policy applies to users of PFM systems.

Policy Statements

1. The data stored in mobile devices shall be backed up frequently and measures provided for recovery in compliance with Backup Policy.
2. The mobile devices shall be used in a manner to ensure separation of private and business/official use in compliance with Acceptable Use Policy and BYOD Policy.
3. Data and communications on the mobile devices shall be encrypted and necessary measures put in place to provide secure communications in compliance with encryption best practice.

4. An inventory of all mobile devices interacting with PFM systems shall be stored electronically and reviewed basing on technical capacity of the devices.
5. All mobile devices owned by MCDAs shall be tagged and an inventory kept as mentioned in (4) above.
6. 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.
7. Mobile devices accessing PFM systems shall have the GPS capabilities enabled to allow location transparency.

This policy shall be used in compliance with the GoK Information Security Standard guidelines on Mobile device Management

Enforcement

MCDAs shall enforce this policy and ensure compliance.

MALWARE MANAGEMENT

Introduction

Attacks on PFM systems and other 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 reduced efficiency, productivity, and service delivery. The PFM Systems are therefore not an exception, and thus the need to have proper mechanisms in place to mitigate these vulnerabilities.

Purpose

The objectives of malware management are to:

1) Outline the requirements/process of mitigating against malware.
2) Mitigate service disruption and restoration caused by malware attacks.
3) Come up with guidelines to sensitize users on malware management

Scope

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

Application

This policy applies to all MCDAs operating PFM systems.

Policy statements

For the Government to achieve business objectives and ensure continuity of its operations, PFM Systems owners shall adopt and follow well-defined and time-tested plans and procedures, to ensure the protection of IT assets from malware and virus attacks.

All computing devices responsible for PFM systems shall be managed as stipulated below.

Policy guidelines

a) Devices shall be installed with licensed antimalware softwares.
b) Anti- malware software shall be regularly updated.
c) Users shall be prevented from accessing, materials from unauthorized sources.
d) Users shall not uninstall /disable antimalware agents or applications in computing devices
e) Where users suspect that their computers have been attacked, their computers shall be isolated until the threat is neutralized
f) Users shall only use authorized accounts and software.

Enforcement

MCDAs shall enforce this policy and ensure compliance.

BRING YOUR OWN DEVICE POLICY

Introduction

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.

Purpose

The purpose of this policy is to guide on secure usage of personal devices to access PFM systems and resources

Scope

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

Application

This policy applies to internal and external stakeholders using PFM systems and resources.

Policy Statements

Use of personal devices to access PFM systems and resources shall be authorized and subject to the guidelines provided in this policy

Policy Guidelines

To ensure the security of PFM systems information, authorized users shall be required to comply with the following.

a) The devices shall be registered before connecting to the network.
b) The devices shall have an up-to date anti-malware software in accordance with the anti-malware policy.
c) Users shall not use unauthorized applications.
d) Use of personal devices shall be regularly reviewed and monitored.
e) The users shall ensure devices are protected from loss, damage or theft.
f) MCDAs shall ensure all work related data on personal devices shall be expunged upon separation of an employee.

Enforcement

The Head of ICT in MCDAs shall enforce this policy and ensure compliance.

SYSTEMS AND APPLICATIONS SECURITY

SYSTEMS ACQUISITION MAINTENANCE AND DECOMMISSIONING

Introduction

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 Systems and applications.

Purpose

The purpose of this policy is to provide guidance on secure Systems acquisition, development, commissioning, maintenance and decommissioning of PFM Systems in-line with the business needs and relevant procurement laws and regulations.

Scope

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

Application

This policy applies to all internal and external stakeholders involved in acquisition, development, commissioning, maintenance and decommissioning of PFM Systems.

Policy Statement

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

Policy guidelines

a) Acquisition of systems shall conform to Government information security standard
b) All vendor supplied defaults for system passwords and other security parameters shall be changed
c) Vendor support for the version of all PFM systems acquired shall be verified and they be appropriately hardened based on developer security recommendations.
d) Software development personnel shall be trained in writing secure code for their specific development environment and responsibilities to reduce dependency on contractors.
e) Static and dynamic analysis tools shall be utilized to verify that secure coding practices are being adhered to for internally developed software.
f) Web application firewalls (WAFs) shall be deployed that inspect all traffic flowing to the web application for common web application attacks.
g) Escrow agreements shall be entered into for safeguarding of source code in the event the system is not fully owned by the MCDA
h) Appropriate change control processes for PFM systems shall be put in place throughout the development lifecycle, coupled with technical reviews of applications for any changes made after operating platform changes.
i) Changes to PFM systems shall be controlled and documented.
j) Outsourced development shall be strictly controlled and monitored to ensure that information security controls are designed and implemented in the application.
k) System security testing shall be regularly conducted throughout system life cycle.
l) System acceptance testing shall be carried out for new systems, upgrades, and newer versions.

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

Maintenance of PFM System

n) All applications shall be maintained regularly to ensure optimal and secure performance

o) All active applications within PFM systems environment shall be monitored using appropriate tools.

p) MCDAs shall maintain separate environments for production and non-production of PFM systems.

Decommissioning of PFM Systems

q) MCDAs shall define acceptable guidelines for identifying systems for decommissioning, ensure decommissioned assets do not retain organizational data and ensure they are removed from active operating environment.

r) A data migration plan shall be developed that incorporates the following elements:

s) An impact analysis;

t) Issue of notification to service providers, users and customers;

u) Issue of notification of decommissioning to all relevant interfaces and interconnections;

v) Timeframe, plan and schedule;

w) Data integrity and validation checks before archiving;

x) Transfer or redeployment of equipment and other assets;

y) Transfer or cancellation of licenses;

z) Removal of obsolete equipment and software;

aa) Removal of obsolete cables and termination equipment;

bb) Removal of any emanation control equipment or security enhancements;

cc) Return or safe disposal of any emanation control equipment or security enhancements;

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

ee) Equipment and media sanitization including any cloud-based data & services

ff) Any legal considerations for supply or service contract terminations

gg) Asset register updates

hh) Retraining or redeployment of support staff.

Enforcement

The Head of ICT shall ensure the enforcement of this policy. Violation of any section of this policy will be treated as misconduct and the necessary disciplinary measures as stipulated in the Public HR manual and other relevant legislation.

APIs AND INTEROPERABILITY

Introduction

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, or APIs, facilitate interoperability by enabling applications to exchange data and functionality easily and securely.

Purpose

The purpose of this policy is to guide secure and effective integration of PFM systems.

Scope

This policy covers the use of APIs to integrate PFM Systems.

Application

This policy applies to all internal and external stakeholders involved in PFM Systems integration.

Policy Statement

Information security shall be applied consistently when implementing APIs and designing interoperability of PFM systems

Policy guidelines

When implementing APIs and designing interoperability of systems the following shall be observed;

a) Standards for message formats between two or more PFM systems shall be harmoniously validated in order to avoid transmission errors.
b) Request parameters of relevant error messaging shall be Validated so as to defend against injection attacks
c) Proper authentication and authorization shall be done to determine messages are from authorized parties only.
d) Controls shall be established to guard against manipulation of data in active transactions and attempts to alter transactions should issue alerts and be recorded.
e) Electronic signatures shall be used to safeguard against non-repudiation of transactions in PFM systems.
f) Data shall be encrypted using the latest technology when on transit
g) All PFM Systems shall be integrated as per government's systems and applications standard

Enforcement

This policy shall be enforced through various methods, including but not limited to, periodic walk-through, internal and external audits.

An employee found to have violated this policy shall be subject to disciplinary action as per Public service HR manual.

VIRTUALIZATION
Introduction

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 allow computing resources to be used more efficiently by a number of different users or applications with different needs.

Purpose

The purpose of this policy is to provide guidance on secure and efficient use of shared resources of PFM Systems through virtualization.

Scope

This policy covers PFM systems deployed in virtualized environments in MCDAs.

Application

This policy applies to internal and externals stakeholders using PFM Systems.

Policy Statement

Processes shall be implemented to evaluate, implement, monitor and manage security within a virtualization environment. Security controls shall include implementation of security controls and procedures granularly at each virtual machine, securing virtual machines, virtual network and other virtual appliances from attacks and vulnerabilities that may surface from the underlying physical device and ensuring control and authority over each virtual machine.

Policy guidelines

In the deployment of virtualization technology implementing agencies shall take into consideration the following:

a) The guest host shall be isolated from the host operating system.
b) Both the host and virtual environment shall only be accessed by authorized user(s).
c) Virtualization software shall be patched as vendor fixes are released.

d) Access and visibility between the guests hosted within the host operating systems shall be restricted
e) Security monitoring of the virtualization software and auditing shall be done to generate reports that flag suspicious configurations and communication between the guests.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

An employee found to have violated virtualization policy shall be subject to disciplinary action as per Public service HR manual.

COMMUNICATION SECURITY

Introduction

This policy document stipulates how the Public Finance Management (PFM) Systems will handle communication between its internal and external stakeholders.

Purpose

The overall objective of this communication 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 their confidentiality, integrity and availability.

The specific objectives of the communication policy are:

- To establish administrative direction, procedural requirements, and technical guidance to ensure the appropriate protection of information when running PFM Systems in a computer network.
- To ensure that a secure method of connectivity is provided between the PFM System owners and PFM System users.

- To provide guidelines for the use of network and computing resources associated with the network connection.

Scope

This policy contains multiple sections i.e. Network Security, Wireless Security, Electronic Messaging, Information Sharing and Agreement on Information Transfer that are in many ways inter-related.

Application

The policies and procedures described in this document shall cover various groups of people. Some policies cover every user of the PFM Systems and its resources, and others apply to specific groups who administer or manage the network.

NETWORK SECURITY

Introduction

Network Security is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility 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.

Purpose

This policy aims to guide on use, protection and security of information in networks while advocating for industry best practices to ensure confidentiality, integrity and availability of the PFM Systems.

Scope

This policy covers all aspects of computer networks infrastructure, configurations, management and use.

Application

The policy shall be applicable to all internal and external stakeholders who utilize any portion of the network or its resources to run or access PFM Systems.

Policy statements

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

Written permission, e-mail or otherwise, from an authorized contact person in the owner agency, shall be attained in order to add new network accounts and/or devices, grant network file rights, search archived e-mail, or install new application software on a PC.

Individual user accounts and passwords are issued to create security for the systems and data. The purpose of a User ID and password is to create security from unauthorized access to the PFM Systems or confidential data.

Approved employees and authorized third parties may utilize the benefits of VPNs, which are a “user managed” service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Policy 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 PFM Systems Administrators shall;

a) Ensure Network Operations related Passwords e.g. switches and routers shall be stored in a secure and password protected management application.
b) Perform regular scans from outside each trusted network perimeter to detect any unauthorized connections which are accessible across the boundary.
c) 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.
d) Deny communication over unauthorized TCP or UDP 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.

e) Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.
f) Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.
g) Enable the collection and monitoring of Network Flows and logging data on network boundary devices.
h) Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.
i) Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.
j) Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.
k) Maintain standard, documented security configuration standards for all authorized network devices.
l) Configure rules that allow traffic to flow through network devices and should be documented in a configuration management system with a specific business reason for each rule.
m) Compare all network device configurations against approved security configurations defined for each network device in use and alert when any deviations are discovered.
n) Install the latest stable version of any security related updates on all network devices.
o) Manage network devices using multi-factor authentication and encrypted sessions where possible.
p) Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.
q) Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.

r) 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.
s) 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 logged.
t) Configure actively connected devices through VPNs shall force all traffic to and from the PC over the VPN tunnel. All other traffic shall be dropped.
u) Automatically disconnect users from the network after prescribed time of inactivity.
v) Limited an absolute connection time of a VPN session to 24 hours.
w) The third party shall be entirely responsible for providing the appropriate security measures to ensure protection of their private internal network and information.
x) By using VPN technology with personal equipment, users shall understand that their machines are a de facto extension of PFM Systems network, and as such are subject to the same rules and regulations that apply.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

WIRELESS SECURITY

Introduction

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 (e.g., personal computers, wireless phones, smart phones, etc.) connected to any of the PFM Systems networks.

Purpose

This policy aims to guide on access and management of wireless networks and computing resources associated with it for PFM Systems connection.

Scope

This policy covers all aspects of wireless networks infrastructure, configurations, management and use.

Application

The policy shall be applicable to all internal and external stakeholders who utilize any portion of the network or its resources to run or access PFM Systems.

Policy statements

All point-to-point (building-to-building) wireless devices shall use PFM Systems -approved vendor products and security configurations. A data encryption method, which meets or exceeds the GoK Information Communication Technology standard, is required.

All wireless access points and base stations shall be registered and approved as set out in GoK Information Communication Technology standard guide. All wireless LAN access must use PFM System-approved vendor products and security configurations. A data encryption method, which meets or exceeds the GoK Information Communication Technology standard, is required. Client authentication must be accomplished using at least two-factor authentication method.

All wireless network interface cards (NIC) (i.e., PC cards) used in a laptop or desktop computers shall be registered and approved by Information Technology. If a mobile device contains both a LAN NIC and wireless NIC, the wireless NIC must be disabled while the device is connected to the internal network via the LAN NIC.

Policy Guidelines

The PFM Systems administrators shall:

a) Maintain an inventory of authorized wireless access points connected to the wired network.
b) Configure network vulnerability scanning tools to monitor, detect and alert on unauthorized wireless access points connected to the wired network.
c) Disable wireless access on devices that do not have a business purpose for wireless access or pose a risk in facilitating adhoc wireless connections (computer to computer), by-passing network controls.
d) Leverage on wireless encryption standards for data in transit.
e) Ensure that wireless networks use authentication protocols that require multi-factor authentication.
f) Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.
g) Scan wireless devices for malware before admission to the network.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

ELECTRONIC MESSAGING

Introduction

Electronic messaging also referred to as electronic mail is an interactive, computer-driven technology that facilitates two-way interpersonal communication among individuals or groups.

Policy Objective

This policy provide guidance and direction for electronic messaging such as e-mail, chat etc. containing confidential and/or protected information that may be passed through PFM systems.

Scope

This policy covers all aspects of electronic messaging as used in the PFM Systems.

Application

The policy shall be applicable to all internal and external stakeholders utilize or pass information using the Electronic Messaging technologies for PFM Systems.

Policy Statement

Security controls shall be established to protect electronic messaging from unauthorized access, modifications or denial of service.

Messages on PFM systems are considered organisation's information assets and as such the PFM Systems owner shall have right to access, control and examine such messages on need basis.

Policy Guidelines

a) 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.
b) PFM Systems Users shall be responsible for encrypting attachments (Microsoft Office, Adobe PDF, etc.) that contain protected and/or

confidential information and validating the recipients email address or other contact information prior to sending any messages.

c) Protected and/or confidential information shall not be entered in the subject line of any electronic message.
d) PFM system users shall not provide their login ID or password to another person or vendor due to potential security risks
e) Auto-forwarding email accounts containing protected information to any external mail service (Google, Yahoo, etc.) shall not be permitted
f) Public electronic message services shall not be used for official communication.
g) PFM system users shall not use their official email accounts for personal matters.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

INFORMATION SHARING

Introduction

PFM 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 Systems for strengthening the legislation and guidance in this area in particular through the Data Protection Act, 2019. It is important that we protect and safeguard person-identifiable information that it gathers, creates processes and discloses, in order to comply with the law and to provide assurance to the public.

Information sharing can take the form of:

a) A reciprocal exchange of data.
b) One or more PFM Systems providing data to a third party or parties.
c) Several PFM Systems pooling information and making it available to each other.
d) Several PFM Systems pooling information and making it available to a third party or parties.
e) Exceptional, one-off disclosures of data in unexpected or emergency situations.

Policy Objective

This policy aim to provide a guideline on the acceptable use of information sharing in PFM systems while ensuring security of such information

Scope

This policy covers all aspects on information sharing as used in the PFM Systems.

Application

The policy shall be applicable to all internal and external stakeholders who share information across PFM Systems and with other entities.

Policy Statement

Cryptographic techniques to protect the confidentiality, integrity and authenticity of information shall implement by all the PFM Systems owners.

Policy Guidelines

a) The PFM Systems Users shall adhere to retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant PFM Policies and regulations.
b) The PFM Systems Users shall adhere to controls and restrictions associated with using communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses.
c) The PFM Systems Users shall take appropriate precautions not to reveal confidential information by for example not leaving messages containing confidential information on answering machines.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

AGREEMENTS ON INFORMATION TRANSFER

Introduction

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.

Policy Objective

This policy strives to provide guidance on management of the transmission, dispatch and control of information undertaken through the PFM Systems.

Scope

This policy covers all aspects of agreements on information transfer as executed in the PFM Systems.

Application

The policy shall be applicable to all internal and external stakeholders who enter into agreements on information transfer between PFM Systems and with other entities.

Policy Statements

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

Policy Guidelines

a) 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 PFM policies, and which control and protect the confidentiality, integrity and availability of such data.

b) Asset Owners shall ensure appropriate mechanisms are implemented and followed to protect transfer of their information.
c) 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.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

INFORMATION SECURITY RISK MANAGEMENT

Introduction

Risk management is the process by which an organization manages risk to acceptable levels within acceptable tolerances, identifies potential risk and its associated impacts, and prioritizes their mitigation based on the organization's business objectives. Risk management develops and deploys internal controls to manage and mitigate risk throughout the organization.

Purpose

To empower the office responsible for information security function to perform periodic information security risk management (ISRM) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Scope

Information Security Risk Assessment shall be conducted on all PFM Systems Operating environment including but not limited to Infrastructure, procedures and personnel.

Policy Statement

The MCDAs operating PFM systems shall develop an information security risk management framework to provide a structured way of risk identification, analysis, and implementation of appropriate risk management procedures.

Risk assessment shall also consider existing legal and regulatory frameworks relevant to the MCDAs mandate that could impact on how it manages information security risks.

Information security shall be addressed in all PFM projects regardless of the type and throughout its life cycle.

Policy Guidelines

a) Information security risk management can be undertaken as part of a broader enterprise risk management approach.

b) The execution, development and implementation of remediation programs shall be the joint responsibility of the Officer responsible for information security and the process owners.
c) Process owners are expected to cooperate fully with any risk assessment being conducted on systems/processes for which they are accountable.
d) Process owners are further expected to work with the Officer responsible for ISRM in the development of a remediation plan.
e) Where appropriate, information assets should be labeled and handled in accordance with their criticality and sensitivity.
f) Information security risk assessment shall be conducted annually and on need basis.

INFORMATION ASSET MANAGEMENT

Introduction

Information asset is data, device, or other component of the environment that supports information-related activities. Assets generally include hardware, software and confidential information.

Information assets include: -

a) an operating system
b) infrastructure
c) business application
d) off-the-shelf product
e) user-developed application
f) records
g) Data and information
h) IT hardware

Purpose

The purpose of this policy is to provide guidance in the management of information assets within PFM systems environment

Scope

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

Application

This policy applies to both internal and external stakeholders that interact with information assets within PFM systems operational environments.

Policy Statement

Information assets shall be acquired, operated, maintained and disposed in consideration of their confidentiality, integrity and availability

Policy Guidelines

a) An inventory of all information assets shall be maintained for PFM systems
b) The information assets shall be appropriately labeled, classified and protected.
c) MCDAs shall define and periodically review access restrictions and classifications to critical assets, considering applicable access control policies;
d) Information assets shall be maintained regularly or as per the manufactures a recommendation and records kept.
e) Proper security of information shall be maintained when the asset is decommissioned, disposed or destroyed.
f) Unauthorized use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) shall be prevented;

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

INFORMATION CLASSIFICATION AND SHARING

Introduction

Information classification is a process in which organization access the data that they hold and the level of protection should be given.

Purpose

This Policy outlines the classification of electronic information, security measures and responsibilities required for securing electronic information and preventing unauthorized destruction, modification, disclosure, access, use, and removal. It also serves as an information security classification reference for other PFM Systems, procedures, standards, organization regulations, or other directives relating to the classification of information.

Scope

There should be an information classification scheme that applies across all PFM systems in the MCDAs, which:used to determine varying levels of confidentiality of information, Provides a description of each level of confidentiality, Considers the potential business impact from the loss of confidentiality of information, Lists examples of information types for each specific classification level.

Application

This Policy must be read in conjunction with the Policy on IT Resources Acceptable Use and IT Security Procedures.

This Policy applies to all electronic information that is in the custody or control of the MCDAs. This Policy does not provide an exhaustive list of safeguards. The Institution shall be responsible for the interpretation of this Policy.

Policy Statement

This policy shall apply to all custodian's/administrators of PFM systems users and other authorized affiliates failure to comply to the policy may result to sanctions.

Policy Guidelines

An information classification scheme should be established to classify:

a) Information stored in physical

b) Information stored in electronic

c) Electronic communications

The information classification scheme should require:

a) That information is protected in line with its assigned level of classification

b) Sign-off of the assigned classification applied to information by the relevant business owner

c) That information classifications are reviewed and updated regularly and when changes are made

The information classification scheme should:

a) Provide guidance on handling requirements for each classification at each stage of the information lifecycle

b) Explain how to handle conflicting classifications

The information classification scheme should take into account requirements for document retention based on the PFM System document a retention policy guided by:

a) Legal and regulatory obligations

b) Business requirements

c) Technical requirements

There should be approved methods for labeling classified:

a) Information stored in paper form

b) Information stored in electronic form

c) Electronic communications

Information classification details should be:

a) Recorded in an inventory, or equivalent

b) Included in agreements with customers, service providers and external suppliers

c) Made widely available

Information classification details recorded should include the:

a) type of information being classified

b) Level of classification of the information

c) Date for reclassification

d) Identity of the information owner

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

BUSINESS CONTINUITY MANAGEMENT

Introduction

This policy provides the framework for disaster recovery and business continuity plan for the PFM systems in case an unplanned event or disaster occurs.

Policy Objectives

The objectives of this policy are as follows:

a) Guide on the initial actions and processes in case of unplanned event or disaster affecting any of the PFM systems
b) Ensure there is continuity and restoration of business operations, functions and services in the event of a disruption or loss of service.
c) Minimize on the impact resulting from the disruption of a PFM system.
d) Protect the PFM systems, associated assets and personnel.

Scope

The policy covers all the PFM ICT resources and personnel that support critical business processes.

Application

The policy applies to all the PFM systems and the associated components that include but not limited to the ICT hardware, software, hosting facilities and personnel.

Policy Statement

The custodians/administrators of PFM systems shall develop, implement, maintain and document Business Continuity Plans, Disaster Recovery Plans, Data Backup and Recovery Plans.

Policy Guidelines

a) The respective custodians/administrators of PFM systems shall develop, implement and maintain Business Continuity Plans (BCPs) which must be aligned with the business need and approved by the business owners. 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.
b) All the respective custodians/administrators of PFM systems shall develop, implement and maintain up to date Disaster Recovery Plans (DRPs) whose configurations must be aligned with the system/application business requirements and approved by the business owners. The DRPs must be tested and reviewed against the approved business requirements on a routine basis.
c) All the respective custodians/administrators of PFM systems shall develop, implement and maintain Back-ups and Recovery Plans whose configurations must be aligned with the system/application business requirements and approved by the business owners. The plans must be tested, audited and documented regularly to ensure that they meet the requirements of the business continuity plans.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

THREAT AND VULNERABILITY MANAGEMENT

Introduction

Threat and Vulnerability Management is the cyclical practice of identifying, assessing, classifying, remediating, and mitigating security weaknesses together with fully understanding root cause analysis to address potential flaws in applications

Purpose

The purpose of this policy is to provide guidance in the remediation of security weaknesses in PFM systems.

Scope

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

Application

This policy applies to all staff managing PFM systems

Policy Statement

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

Policy guidelines

a) 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;
b) Timelines shall be defined to react to notifications of potentially relevant technical vulnerabilities;
c) Once a potential technical vulnerability has been identified, the MCDA shallidentify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems or applying other controls;
d) 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;
    d. Raising awareness of the vulnerability;

e) 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;
f) MCDAs shall prohibit the use of unauthorized software and implement controls that prevent or detect the use of unauthorized software and suspected malicious websites.
g) The organization shall define and enforce strict policy on which types of software users

may install and identify and document what types

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

DISASTER RECOVERY PLAN Policy

Introduction

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives MCDAs a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by MCDAs that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

Policy

Contingency Plans

The following contingency plans must be created:

a) Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
b) Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.

c) Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
d) Criticality of Service List: List all the services provided and their order of importance.
e) It also explains the order of recovery in both short-term and long-term timeframes.
f) 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.
g) 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.
h) Mass Media Management: Who is in charge of giving information to the mass media?
i) Also provide some guidelines on what data is appropriate to be provided.
j) After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.
k) The plan, at a minimum, should be reviewed an updated on an annual basis.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

HUMAN RESOURCES SECURITY

Introduction

The aim of the document is to provide Public Finance Management Reforms Information Systems users with guidelines and requirements regarding human resources security policy and its objective is to ensure that all employees (including contractors and any user of sensitive data) are qualified for and understand their roles and responsibilities of their job duties and that access is removed once employment is terminated.

Policy objective

The objective of this policy is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

To bring harmony in the workplace.

To promote effective communication among appraise and supervisor

Scope

This policy applies to all personnel and contractors accessing data and systems, during employment, termination or change and contractors providing services during the period of their contract.

Application

This policy applies to all MCDAs staff and contractors that are engaged in PFM systems.

Policy statement

MCDA ensure all employees of and contractors who are involved in systems and data are aware of, understand, and fulfill their responsibilities in regards to information security.

Policy guidelines

Manage your human resource security in the following ways:

a) Provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
b) Ensure that employees and contractors are aware of and fulfil their information security responsibilities.

c) Protect the organisation's interests as part of the process of changing or terminating employment.

BACKGROUND SCREENING

Policy statement

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

Policy guidelines

a) MCDA shall conduct background verification checks on all candidates for employment in accordance with relevant laws, regulations and ethics.
b) The screening shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
c) Internal promotions that involves the person accessing mission critical assets shall also attract further and more detailed vetting
d) MCDA shall have contractual agreements (code of conduct) with their employees and contractors that reflect the organization's policies for information security

IN-SERVICE

Policy statement

All MCDAs staff running PFMR systems shall ensure that all employees and contractors are aware of, understand, and fulfill their responsibilities in regards to information security.

Policy guidelines

a) MCDAs running PFMR systems are provided with guidelines to state information security expectations of their role within the organization;
b) MCDAs staff to conform to the terms and conditions of employment, which includes the organization's information security policies and appropriate methods of working;
c) MCDAs are provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing").
d) There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an

information security breach.

TERMINATION OR CHANGE OF RESPONSIBILITIES

Policy statement

To protect the MCDAs interest as part of the process of changing or terminating employment, it shall seek to ensure that during this process, human resource information security is not compromised.

Policy guidelines

a) To prevent unauthorized access to sensitive information, access must be revoked immediately upon termination/separation of an employee with access to such information. This also includes the return of any assets of the organization that was held by the employee.
b) Termination or change of responsibilities is communicated appropriately to all relevant functions and authorities.
c) All access rights issued shall be disabled or reassigned in accordance to the access control policy
d) Duties and responsibilities on the employees, who have designated or transferred, shall be delegated or allocated to another employee appointed by the MCDAs.
e) Responsibilities and duties that remain valid after termination or change or employment shall be defined, communicated to the employee and enforced.
f) The MCDAs should introduce an NDA agreement from the beginning to keep reminding the staff.

INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

Policy statement

The information security awareness program should aim to make employees and, where relevant, contractors aware of their responsibilities for information security and the means by which those responsibilities are discharged.

Policy guidelines

a) MCDAs staff shall conduct an information security awareness programme in line with the organization's information security policies and relevant procedures, taking into consideration the organization's

information to be protected and the controls that have been implemented to protect the information.

b) The awareness programme shall be planned taking into consideration the employees' roles in the organization, and, where relevant, the organization's expectation of the awareness of contractors.
c) Information security education and training shall take place annually. Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not just to new starters and should take place before the role becomes active.
d) An assessment of the employees' understanding shall be conducted at the end of an awareness, education and training course to test knowledge retention and understanding.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

OPERATIONAL SECURITY

Information and Communications Technology includes all activities that ensure appropriate resource management procedures, specifically relating to information and communications technology (ICT).

ACCESS CONTROL POLICY

Access control is a fundamental component of information security that dictates who's allowed to access and use PFM systems and assets. Through authentication and authorization, access control policies make sure users are appropriately identified and have the right level of access.

Logical Access Control Policy

Scope

This policy covers logical access to all servers, applications, databases or network devices that contain or process PFM systems and information.

Purpose

The purpose of this policy is to provide guidance on the design of access controls to minimize potential exposure to PFM systems resulting from unauthorized use of resources and to preserve and protect the confidentiality, integrity and availability of network devices, databases and applications.

Policy Statement

Access to PFM systems and resources shall be based on least privilege and the need-to-know basis

Policy guidelines

a) A formal procedure shall be developed to guide the process of granting and revoking access to PFM systems.
b) Access rights and privileges to PFM systems shall be assigned based on user's roles and responsibilities on the respective systems and applications.
c) User access passwords shall conform to the password policy.
d) All PFM systems shall have audit logs to track user's activity. The logs shall be monitored regularly.
e) Remote access to the systems shall be allowed through an authorized secure connection.
f) Periodic audits of access controls and user rights shall be conducted to ensure they are working as expected.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

CLOUD SECURITY

Introduction

Cloud computing is a concept that refers to services, applications, and data storage delivered online through remote servers that are connected through the internet. Cloud computing services can be offered through the following service models: Software As A Service (SaaS), Platform As A Service (Pass) or Infrastructure As A Service (IaaS).

Further, the cloud offerings can be classified based on the sharing of the infrastructure as either Private, Public, Community or Hybrid cloud.

Purpose

The purpose of this policy is to provide guidance for secure acquisition and deployment of cloud based PFM systems.

Scope

This policy covers the acquisition and deployment of cloud based PFM systems

Application

This policy applies to internal and external stakeholders using PFM systems.

Policy statement

In order to enhance efficiency, cloud computing shall be adopted for PFM systems in conformity to Government information security standards and applicable legislation.

Policy guidelines

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

a) To mitigate against risks associated with vendor lock-in, the Head of ICT shall prepare an exit strategy as part of procurement and contracting with the Cloud Service Provider.
b) Management of identifiable citizen data shall be subject to the provisions of the Kenya Data Protection Act, 2019.
c) Licensing needs shall be projected over a period and ensure the cloud provider meets those needs.

d) Adequate safeguards shall be put in place to secure authentication, authorization and other identity and access management functions, and are suitable for the organization.
e) 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. Requirement for data sanitization from storage media, electronic and physical access rights be revoked from the cloud provider, and assets provided to the provider returned or, if not possible, be securely purged.
    c. Non-Disclosure Agreement (recommended before provisioning any service)
    d. Full disclosure in case of breaches to regulated information.
    e. Ownership for 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 requirements
    i. Service management processes
    j. Audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle
    k. The application of appropriate Government retention policies
    l. A clear process documenting the responsibilities of each party with respect to extracting and destroying data

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

CHANGE MANAGEMENT

Introduction

New ICT solutions can be highly disruptive to an organization. Well executed change management initiatives ensure smooth transition to new work processes thus eliminating interruptions to organization's operations.

Purpose

The purpose of this policy is to guide the process of instituting changes in the PFM systems operational environment in order to ensure that they are carried out in a planned manner to minimize negative impact to services.

Scope

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

Application

This policy applies to internal and external stakeholders who are involved or are affected by the changes in the PFM systems environment.

Policy Statement

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

Policy Guidelines

a) All changes shall be planned and communicated to all relevant parties
b) A documented procedure shall be documented for initiation of changes. The procedure shall clearly define the roles to the process owner and approver of the changes in line with Government information security standards
c) A request for changes shall contain sufficient information to enable the evaluation of the potential risks and benefits.
d) A roll-back plan shall be developed and implemented before the change is carried out.
e) Changes shall be tested in a test environment before implementation.
f) Changes shall be effected at a time that will minimize disruption to service delivery.

g) Users shall be notified on the results of the change once the changes are complete.
h) Users shall be taken through formal training on the new operational processes impacted by the change.
i) Users shall review and accept completion of the changes and readiness for transition to production environment; the review shall be documented.
j) A log of all relevant information on the changes shall be retained

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

USER ACCOUNT MANAGEMENT Policy

Introduction

There is need to carefully manage all user accounts, especially those accounts that have unlimited (administrative) rights on that computer. Administrative rights are needed in order to install software and alter most configuration settings. These powerful capabilities make accounts with administrative rights prime targets for attackers.

Purpose

To establish the rules for the creation, use, monitoring, control and removal of user accounts and ensure that all approved users are created using the principle of least privilege

Scope

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

Application

Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special

access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

Policy Statement

All authorized users of PFM systems shall have accounts created for them in accordance with this policy. Privileged and special access accounts shall be granted only in accordance with this policy.

Policy Guidelines

a) Supervisors should formally make requests for user account creation for their staff to the relevant ICT Section Head for approval.
b) All user accounts must be uniquely created. The first three characters of an account are prefixed 'pfm' followed by staff number, with exception of service accounts that have the 'pfm' prefix then followed by the service name. Contractors' accounts shall have the contractor's ID number.
c) User accounts that are unused or inactive for thirty days are automatically locked or disabled.
d) Users shall be granted privileges that are commensurate with their roles and responsibilities in the PFM systems.
e) MCDAs departments must submit to PFM ICT Head a list of administrative contacts for their systems that are connected to the PFM network.
f) All users of Administrative/Special access accounts must have account management instructions, documentation, training, and authorization.
g) Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege.
h) Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate for work being performed (e.g. user account vs. administrator account).
i) Employees who need administrative powers on a particular computer should be assigned two accounts: one with administrative rights and another that has only limited privileges. These employees should be trained to log in under their limited account to perform routine daily duties and to log in to their administrative account only when they need to perform some action, such as installing new software, which requires administrative rights.
j) Each account used for administrative/special access must meet the PFM Password Policy.

k) The password for a shared administrator/special access account must change when an individual with the password leaves the department or PFM or upon a change in the vendor personnel assigned to the PFM contract.
l) 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 situation e.g. via use of securely kept password envelopes.
m) When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they must be:
   - authorized;
   - created with a specific expiration date;
   - Removed when work is complete.
n) All non-PFM users (special access accounts) must sign a PFM Non-Disclosure Agreement (NDA) before account access is enabled.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

PASSWORD POLICY

Introduction

Passwords are the primary means of providing user access to system resources. Once a particular resource is compromised, other systems can be compromised as well, resulting in the possibility of disclosure of organizational and personal information. To prevent information theft, users must ensure the confidentiality of all passwords used to connect to PFM systems.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

To authenticate and authorize users of the PFM Systems and ensure that only legitimate users can access the system.

Scope

The policy covers all users who access the PFM systems

Policy statement

Every user accessing the PFM Systems should be identified using a password

Policy Guidelines

a. Passwords shall be used on all PFM automated information systems to uniquely identify individual users.
b. Be at least six characters in length.
c. Password complexity design shall be incorporated in all PFM systems to include at least two of the following: upper case, lower case, special characters and numbers.
d. Passwords should not be shared amongst users. Generic, system defaulted or group passwords shall not be used. Password history should be set to the last 3 passwords in all ICT systems.
e. To preclude password guessing, an intruder lock-out feature shall suspend accounts after three invalid attempts to log on; manual action by an administrator after user verification is required to reactivate the account.
f. Passwords shall expire after every 90 days.
g. Not be dictionary words.
h. Not be portions of associated account names (e.g. user ID, log-in name, personal information).
i. Not be character strings (e.g. abc or 123).
j. Not be simple keyboard patterns (e.g. QWERTY, asdf).

k. In addition, users are required to select a new password immediately after their initial log in.
l. Users are responsible for the security of their password(s) and are accountable for any misuse.
m. Incidents where a user suspects that his/ her accounts has been compromised shall immediately be reported to the IT Security.
n. Any default passwords must be changed on all systems prior to connection to any network, even in pre-deployment testing.
o. Screen-saver password must be enabled after 5 minutes of inactivity of the user. Users must not be allowed to change the inactivity time.
p. Vendor or service accounts will be removed from computer systems prior to deployment and new passwords are to be implemented on all systems immediately upon installation at PFM facilities.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

PHYSICAL AND ENVIRONMENTAL SECURITY

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

Purpose
This policy provides the guidance for the physical protection of ICT resources within the PFM systems environment.

Scope
This policy covers all information processing facilities for PFM systems

Application
This policy applies to all internal and external stakeholders who use PFM systems.

Policy statement
MCDAs shall ensure protection of critical and sensitive PFM systems information processing facilities.

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

a) Removable media (flash disks, portable hard drives) should be securely stored when not in use. If they contain highly sensitive or confidential data, they must be locked up.
b) Removable media should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
c) MCDAs shall ensure installation of clean power to protect ICT equipment from damage.
d) Employees shall not take ICT equipment out of the offices without an approved gate pass duly authorized by their Head of Department and the Head of ICT.
e) Employees should exercise care to safeguard the valuable electronic equipment assigned to them failure to which they should be held accountable.
f) MCDAs shall ensure ICT facilities are hosted within physically and environmentally secured areas.
g) MCDAs shall deploy surveillance and monitoring mechanisms to cover all critical ICT equipment installations.
h) MCDAs shall restrict access to critical ICT installations to authorized personnel.

i) Access rights to secure areas shall be reviewed, updated and/or revoked as and when necessary.
j) Installation, disconnection, modification or relocation of ICT equipment shall only be performed with authority of Head of ICT .
k) Unattended laptops should be secured appropriately.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.

INCIDENT RESPONSE PLAN Policy

Introduction

A Security Incident Response Plan (SIRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited).

Purpose

The purpose of this policy is to establish the requirement that all MCDAs supported by the InfoSec team develop and maintain a security response plan. This ensures that security incident management team has all the necessary information to formulate a successful response in case of a specific security incident.

Scope

This policy applies to any established and defined business unit or entity within the MCDAs that manage PFM systems.

Policy statement

The development, implementation, and execution of a Security Incident Response Plan (SIRP) shall be the primary responsibility of the specific business unit for whom the SIRP is being developed in cooperation with the ICT/InfoSec team.

Business units should properly facilitate the SIRP applicable to the service or products they are held accountable. The business unit security coordinator or champion is further expected to work with the organizational information security unit in the development and maintenance of a Security Response Plan.

Policy guidelines

a) Service or Product Description

The product description in an SIRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

b) Contact Information

The SIRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the

impact to customer. The SIRP document must include all phone numbers and email addresses for the dedicated team member(s).

c) 4.3 Triage

The SIRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

d) Identified Mitigations and Testing

The SIRP must 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.

e) Mitigation and Remediation Timelines

The SIRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

Enforcement

MCDAs information security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits.