THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE, RECORDS AND ARCHIVE MANAGEMENT DEPARTMENT

INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY POLICY

December, 2020

P.O.Box 2006, Dar es Salaam-TANZANIA
Tel: +255 22 215 2875
Email: ramd@nyaraka.go.tz / info@nyaraka.go.tz
Website: https:www.nyaraka.go.tz

TABLE OF CONTENTS

CHAPTER ONE

GROSSARY AND ACRONYMS

1.1 Glossary

TERM	Definition
Authorisation / Authorised:	Official PO-RAMD approval and permission to perform a particular task.
PO-RAMD Network:	The data communication system that interconnects different wired and wireless PO-RAMD Local Area Networks (LAN) and Wide Area Networks (WAN).
Disaster Recovery Plan (DRP)	A master plan specifically developed for an organization describing how to deal with the potential disaster to its information systems. Other related terms include business continuity plan (BCP), business process contingency plan (BPCP) or disaster recovery and business continuity plan (DRBCP)
ICT Assets	Any computer, software, hardware (servers, systems, networks, computers, data communications and telephones) and all other ICT equipment used by and under control of the agency.

ICT Security Policy	A document that elaborate on the Public Agency's ICT Management Philosophy by providing general statements of purpose, direction and required activities for the ICT Security management Framework, commonly known as ICT Security Policy of an Agency.
ICT Security Single Point of Contact	ICT staff appointed that delivers advanced threat detection, incident response and compliance management to ICT Security policy
Information Availability	Assurance that information systems responsible for delivering, storing, and processing information are accessible when needed by those who need them.
Information	Any data in an electronic format that is capable of being processed or has already been processed.
Information Confidentiality	Assurance that information is shared only among authorized persons.
Information and Communication Technology(I.T.) resources:	Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames

	and passwords, and information and data that are owned or leased by PO-RAMD .
Information and Communication Technology(IT)	Embraces the use of computers, telecommunications and office systems technologies for the collection, Processing, storing, packaging and dissemination of information.
Information Owner	The individual responsible for the management of a PO-RAMD directorate or service (e.g. Director of Companies and Business Names, Director of Intellectual Property, Chief Accountant
Information Security:	The preservation of confidentiality, integrity and availability of information.
Information System:	A computerized system or software application used to access, record, store, gather and process information.
Integrity:	Ensuring the accuracy and completeness of information and associated processing methods.
IT Policy	A document that elaborate on the Public Agency's ICT Management Philosophy by providing general statements of purpose, direction and required activities for the entire ICT Management Framework,

	commonly known as ICT Policy of an Agency.
Process / Processed / Processing:	Performing any manual or automated operation or set of operations on information including: Obtaining, recording or keeping the information; Collecting, organizing, storing, altering or adapting the information; Retrieving, consulting or using the information; Disclosing the information or data by transmitting, disseminating or otherwise making it available; Aligning, combining, blocking, erasing or destroying the information.
Risk:	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

Third Party Commercial Service Provider:	Any individual or commercial company that have been contracted by the PO-RAMD to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, and management services etc.) to PO-RAMD .
Threat	A potential cause of an incident that may result in harm to a system or organization.
Users:	Any individual using any of the PO-RAMD's ICT. Resources.

1.2 Acronyms

SLA Service Level Agreement

PO-RAMD President Office, Records and Archives Management Department

ICT – Information & Communication Technology

SPOC – Single Point of Contact

CHAPTER TWO

OVERVIEW

2.1 Introduction

The use of computer systems and the exchange of information electronically have increased rapidly in the area of Public Service Delivery. Within the PO-RAMD there is a growing reliance on computer systems to facilitate the registrations and post registrations activities of the agency, expand communications to our customers and other stakeholders, and improve management and control. This growing dependence comes at a time when the number of threats and actual attacks on these computer systems is constantly increasing.

PO-RAMD information and technology assets are highly valuable and must be closely safeguarded. Information is one of our most important assets and each one of us has a responsibility to ensure the security of this information. Accurate, timely, relevant and properly protected information is essential to the successful operation of PO-RAMD in the provision of services to our customers.

To ensure the continued protection of the agency's information and to maintain a secure environment, the management team of PO-RAMD strongly believes that an ICT security approach aligned with industry standards is necessary.

This policy is mandatory and by accessing any Information and Communication Technology (ICT) resources which are owned or leased by PO-RAMD, users are agreeing to abide by the terms and conditions of this policy.

2.2 Rationale

PO-RAMD operates in a growing electronic, interconnected, and regulated environment that necessitates a consistent and standardized approach to securing technologies and information assets. It is the mandate of PO-RAMD that the information assets are protected from threats, whether internal or external, deliberate or accidental; it is the policy of PO-RAMD to:-

- Implement human, organizational, and technological security controls to preserve the confidentiality, availability and integrity of its information systems and the information held therein;
- Develop and maintain appropriate policies, procedures and guidelines to effect a high standard of ICT security, reflecting industry best practices;
- Monitor, record and log all activities on the PO-RAMD network and use of its ICT resources include internet usage;
- Comprehensively assess and manage risks to PO-RAMD information systems and the information held therein;
- Continuously review and improve PO-RAMD ICT security controls, and rapidly determine the cause

of any breach of security and minimize damage to information systems should any such incident occur;

- Comply with all laws and regulations governing ICT security; and
- Establish ICT security training and awareness initiatives within PO-RAMD.

2.3 Purpose

The purpose of this ICT Security Policy and its supporting policies, standards and guidelines is to define the security controls necessary to safeguard PO-RAMD information systems and ensure the security of the information held therein.

This ICT Security Policy is the cornerstone of PO-RAMD ICT security strategy, aimed at securing the ICT assets of the Agency. It is also the purpose of this document to outline the roles and responsibilities of relevant stakeholders that implement the security controls.

2.4 Scope

This policy applies to all PO-RAMD staff and contractors that use the agency's ICT resources and/or process information on behalf of PO-RAMD. This policy is applicable to information assets owned or leased by PO-RAMD or to devices that connect to PO-RAMD networks or reside at PO-RAMD sites.

In addition to this policy, there will be developed a number of supporting PO-RAMD policies, standards and guidelines to accompany this security document. Each of these accompanying policies, standards and guidelines will be published after appropriate approvals and will cover a specific area of ICT security.

CHAPTER THREE

POLICY STATEMENTS

3.1. ICT Security Governance and Management

3.1.1. Management of ICT Security

3.1.1.1. Single Point of Contact (SPOC) for ICT security Matters shall be appointed.

3.1.1.2. There shall be an ICT Security Strategy incorporated in the agency's ICT Strategy.

3.1.1.3. PO-RAMD **shall** allocate sufficient resources for effective ICT security management.

3.1.2. ICT Security Risk Management

3.1.2.1. PO-RAMD **shall** integrate ICT security risk management (risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and evaluation) into the Agency's Risk Management Framework.

3.1.3. ICT Security Policies

3.1.3.1. PO-RAMD **shall** define a set of policies for ICT security, which shall be approved by management, published and communicated to employees and relevant external parties.

3.1.4. Review of the ICT Security Policies

3.1.4.1. The ICT security policies shall be reviewed after every three years or if significant changes occur, to ensure their continuing suitability, adequacy and effectiveness.

3.1.5. ICT Security Roles and Responsibilities

3.1.5.1. PO-RAMD **shall** define and allocate all ICT security responsibilities.

3.1.6. Segregation of Duties

3.1.6.1. Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Agency's ICT assets.

3.1.7. Contact with Authorities

3.1.7.1. PO-RAMD **shall** maintain appropriate contacts with relevant authorities.

3.1.8. ICT Security in ICT Project Management

3.1.8.1. PO-RAMD **shall** ensure that ICT security is addressed in ICT related projects.

3.1.9. Mobile Devices and Teleworking

3.1.9.1. PO-RAMD **shall** adopt a guideline and supporting ICT security measures to manage the risks relating to mobile devices.

3.1.9.2. PO-RAMD **shall** implement a guideline and supporting ICT security measures to protect information accessed, processed or stored at teleworking sites.

3.2. ICT Security Operations

3.2.1. Documented Operating Procedures

3.2.1.1. Operating procedures shall be documented and made available to all users who need them.

3.2.2. Change Management

3.2.2.1. Changes to the Department, business processes, network configurations, information processing facilities and systems that affect ICT security shall be controlled.

3.2.3. Capacity Management

3.2.3.1 The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

3.2.4. Separation of Development, Testing and Operational Environments

3.2.4.1 Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

3.2.5. Protection from Malware

3.2.5.1. Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

3.2.6. Information Backup

3.2.6.1. Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed Backup policy.

3.2.7. Event Logging and monitoring

3.2.7.1. Event logs recording user activities, exceptions, faults and ICT security events shall be produced, kept and regularly reviewed.

3.2.8. Protection of Log Information

3.2.8.1. Logging facilities and log information shall be protected against tampering and unauthorized access.

3.2.9. Administrator and Operator Logs

3.2.9.1 System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

3.2.10. Clock Synchronization

3.2.10.1. The clocks of all relevant information processing systems within PO-RAMD shall be synchronized to a single reference time source.

3.2.11. Installation of Software on Operational Systems

3.2.11.1. Procedures shall be implemented to control the installation of software on operational systems.

3.2.12. Management of Technical Vulnerabilities

3.2.12.1. Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

3.2.13. Restrictions on Software Installation

3.2.13.1. Guidelines governing the installation of software by users shall be established and implemented.

3.2.14. Information Systems Audit Controls

3.2.14.1. ICT audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes

3.2.15. Network Controls

3.2.15.1. Networks shall be managed and controlled to protect information in systems and applications.

3.2.16. Security of Network Services

3.2.16.1. Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, irrespective of whether these services are provided in-house or outsourced.

3.2.17. Segregation in Networks

3.2.17.1. Groups of information services, users and information systems shall be segregated on networks.

3.2.18. Information Transfer Policy and Procedures

3.2.18.1 Formal transfer guidelines, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

3.2.19. Agreements on Information Transfer

3.2.19.1. Agreements shall be signed with relevant stakeholders to address the secure transfer of business information between the agency and external parties.

3.2.20. Electronic Message Management

3.2.20.1. Information involved in electronic messaging shall be appropriately protected.

3.2.21. Confidentiality and Non-Disclosure Agreements

Requirements for confidentiality or non-disclosure agreements reflecting PO-RAMD needs for the protection of information shall be identified, regularly reviewed and documented.

3.3 Security of ICT Assets

3.3.1. Inventory of ICT Assets

3.3.1.1. ICT assets associated with information and information processing facilities at PO-RAMD shall be identified and an inventory of these assets should be drawn up and maintained.

3.3.2. Ownership of ICT Assets

3.3.2.1. ICT assets maintained in the inventory shall be owned by the relevant function or person at PO-RAMD.

3.3.3. Acceptable Use Policy for ICT Assets

3.3.3.1. Acceptable use policy of information, assets associated with information and information processing facilities shall be identified, documented and implemented.

3.3.4. Return of ICT Assets

3.3.4.1. All employees of PO-RAMD and external party users must return all PO-RAMD ICT assets in their possession upon transfer/termination of their employment, contract or agreement.

3.3.5. Information Management

3.3.5.1. Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

3.3.6.1 An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by PO-RAMD.

3.3.7. ICT Assets Management

3.3.7.1. Procedures for handling ICT assets shall be developed and implemented in accordance with the information classification scheme adopted by PO-RAMD.

3.3.8.1. Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by PO-RAMD.

3.3.9.1. Media shall be disposed off securely when no longer required, using the formal procedures established at PO-RAMD **as** per government directives.

3.3.10.1. Media containing information shall be protected against unauthorized access, misuse or corruption during transportation in and out of PO-RAMD.

3.3.11. Cryptographic Controls

3.3.11.1 PO-RAMD **shall** develop and implement cryptographic controls for protection of information and information processing facilities.

3.4. Identity and Access Management

3.4.1. Access Control Policy

3.4.1.1. Access Control guideline shall be established, documented and reviewed based on business and ICT security requirements of PO-RAMD.

3.4.1.2. Remote access control guideline shall be established and documented as ICT security requirement of PO-RAMD.

3.4.2. Access to Networks and Network Services

3.4.2.1. Users at PO-RAMD shall only be provided with access to the network and network services that they have been specifically authorized to use.

3.4.3. User Registration and De-registration

3.4.3.1. A formal user registration and de-registration process shall be implemented at PO-RAMD **to** enable and disable assignment of access rights.

3.4.4. User Access Provisioning

3.4.4.1 A formal user access provisioning process shall be implemented at PO-RAMD **to** assign and revoke access rights for all user types to all systems and services.

Management of Privileged Access Rights

3.4.5.1 The allocation and use of privileged rights shall be restricted and controlled

3.4.6 Management of Secret Authentication Information of Users

3.4.6.1 The allocation of secret authentication information shall be controlled through a formal management process.

3.4.7. Review of Access Rights

3.4.7.1. All ICT asset owners at PO-RAMD shall review users' access rights at regular intervals.

3.4.8. Removal or Adjustment of Access Rights

3.4.8.1. The access rights of all staff at PO-RAMD and external party users to information and information processing facilities shall be removed upon transfer; termination of their employment, contract or agreement; or adjusted upon change.

3.4.9. Information Access Restriction

3.4.9.1. Access to information and application system functions shall be restricted in accordance with the Access Control Policy of PO-RAMD.

3.4.10. Secure Log-on Procedures

3.4.10.1. Where required by the Access Control Policy, access to systems shall be controlled through a secure log-on procedure.

3.4.11. Password Management System

3.4.11.1. Password management systems must be interactive and must ensure usage of strong passwords.

3.4.12. Use of Privileged Utility Programs

3.4.12.1. The use of utility programs that might be capable of overriding system and application controls must be restricted and tightly controlled.

3.4.13. Access Control to Program Source Code

3.4.13.1 Access to program source code shall be restricted.

3.5. ICT Security Incident Management

3.5.1. Responsibilities and Procedures

3.5.1.1. Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

3.5.2. Reporting ICT Security Events

3.5.2.1 ICT security events shall be reported through appropriate management channels as quickly as possible.

3.5.3. Reporting ICT Security Weaknesses

3.5.3.1. Employees and contractors using the PO-RAMD information systems and services shall be required to note and report immediately after any observed or suspected ICT security weaknesses in systems or services.

3.5.4. Assessment of and Decision on ICT Security Events

3.5.4.1. ICT security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

3.5.5. Response to ICT Security Events

3.5.5.1. ICT security incidents shall be responded to in accordance with the documented procedures.

3.5.6. Learning from ICT Security Incidents

3.5.6.1. Knowledge gained from analysing and resolving ICT security incidents shall be used to reduce the likelihood or impact of future incidents.

3.5.7. Collection of Evidence

3.5.7.1 PO-RAMD **shall** define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

3.6. Systems Continuity Management

3.6.1. Planning ICT Security Continuity

3.6.1.1. PO-RAMD **shall** determine its requirements for ICT security and the continuity of ICT security management in adverse situations, e.g. during a crisis or disaster.

3.6.2. Implementing ICT Security Continuity

3.6.2.1. PO-RAMD **shall** establish, document, implement and maintain processes, procedures and controls (BCP) to ensure the required level of continuity for ICT security during an adverse situation.

3.6.3. Verify, Review and Evaluate ICT Security Continuity

3.6.3.1. PO-RAMD **shall** verify the established and implemented ICT security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

3.6.4. Availability of Information Processing Facilities

3.6.4.1 Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

3.7. Security of ICT Acquisition, Development and Maintenance

3.7.1. ICT Security Requirements Analysis and Specification

3.7.1.1 The ICT security related requirements shall be included in the requirements for new information systems or enhancements to existing information system

3.7.2 Securing Application Services on Public Networks

3.7.2.1 Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

3.7.3. Protecting Application Services Transactions

Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

3.7.4 Secure Development Policy

A policy for secure development of software and systems shall be established and applied to developments within the agency.

3.7.5 System Change and Control Procedures

3.7.5.1 Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

3.7.6 Technical Review of Applications after Operating Platform Changes

3.7.6.1 When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on agency's operations or ICT security.

3.7.7. Restrictions on Changes to Software Packages

3.7.7.1. Modifications to software packages shall be discouraged, limited to necessary changes and all changes should be strictly controlled.

3.7.8. Secure System Engineering Principles

3.7.8.1. Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

3.7.9. Secure Development Environment

3.7.9.1 PO-RAMD **shall** establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

3.7.9.2 PO-RAMD shall perform ICT security assessment in collaboration with e-Government Authority, before deployment of any developed or acquired application software.

3.7.10. Outsourced Development

3.7.10.1. PO-RAMD **shall** supervise and monitor the activity of outsourced system development include Cloud computing.

3.7.11. System Security Testing

3.7.11.1. Testing of security functionality shall be carried out during development.

3.7.12. System Acceptance Testing

3.7.12.1. Acceptance testing programs and related criteria shall be established for new Information systems, upgrades and new versions.

3.7.13. Protection of Test Data

3.7.13.1 Test data shall be selected carefully, protected and controlled.

3.8. Human Resources Security

3.8.1 Screening

3.8.1.1 Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and perceived risks.

3.8.2 Terms and Conditions of Employment

3.8.2.1 The contractual agreements with employees and contractors shall state the employee's and PO-RAMD responsibilities for information security.

3.8.3 Management Responsibilities

3.8.3.1. Management shall require all employees and contractors to apply information security in accordance with the established policy of PO-RAMD.

3.8.4 ICT Security Awareness, Education and Training

3.8.4.1 All employees of PO-RAMD and contractors shall receive appropriate awareness education and training and regular updates in PO-RAMD ICT security policy, as relevant to their job function

3.8.5 Disciplinary Process

3.8.5.1 There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an ICT security breach.

3.8.6 Termination or Change of Employment Responsibilities

3.8.6.1 ICT security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to all employees and contractors of PO-RAMD, and shall be enforced.

3.9. Physical and Environmental Security

3.9.1. Physical Security Perimeter

3.9.1.1 Security perimeters shall be defined and used to protect information processing facilities and areas that contain either sensitive or critical information.

3.9.2 Physical Entry Controls

3.9.2.1 Secured areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

3.9.3 Securing Offices, Rooms and Facilities

3.9.3.1 Physical security for offices, rooms and facilities shall be designed and applied.

3.9.4 Protecting Against External and Environmental Threats

3.9.4.1 Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

3.9.5. Working in Secure Areas

3.9.5.1. PO-RAMD **shall** design and apply procedures for working in secure areas.

3.9.6. Delivery and Loading Areas

3.9.6.1. Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

3.9.7. Equipment Sitting and Protection

3.9.7.1. Equipment shall be identified and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized Access.

3.9.8. Supporting Utilities

3.9.8.1. Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

3.9.9. Cabling Security

3.9.9.1 Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

3.9.10 Equipment Maintenance

3.9.10.1 Equipment shall be properly maintained to ensure its continued availability and integrity.

3.9.11 Removal of ICT Assets

3.9.11.1 Equipment, information or software shall not be taken off-site without prior authorization.

3.9.12 Security of Equipment and Assets Off-premises

3.9.12.1 Security shall be applied to off-site ICT assets taking into account the different risks of working outside PO-RAMD premises.

3.9.13 Secure Disposal or Re-use of Equipment

3.9.13.1 All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

3.9.14 **Unattended User Equipment**

Users at PO-RAMD shall ensure that unattended equipment has appropriate protection.

3.9.15 **Clear Desk and Clear Screen Guideline**

3.9.15.1 A clear desk guideline for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

3.10 ICT Security Compliance and Audit

3.10.1. Identification of Applicable Legislation and Contractual Requirements

3.10.1.1. All relevant legislative statutory, regulatory, contractual requirements and PO-RAMD approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and for PO-RAMD.

3.10.2. Intellectual Property Rights

3.10.2.1. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

3.10.3. Protection of Records

3.10.3.1 Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.

3.10.4. Privacy and Protection of Personally Identifiable Information

3.10.4.1 Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

3.10.5 Independent Review of ICT Security

3.10.5.1 PO-RAMD approach to managing information security and its implementation (i.e. control objectives, controls, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

3.10.6 Compliance with ICT Security Policy and Standards

3.10.6.1. PO-RAMD shall ensure that regular reviews are done, on the compliance of information processing and procedures with the appropriate ICT security policy, standards and any other ICT security requirements.

3.10.7 Technical Compliance Review

3.10.7.1 Information systems shall be regularly reviewed for compliance with thePO-RAMD information security standards and guidelines.

SECTION FOUR

IMPLEMENTATION, REVIEWS AND ENFORCEMENT

4.1. Implementation and Reviews

4.1.1. This policy will be reviewed and updated every three years or more frequently if necessary, to ensure that any changes to the PO-RAMD's organization structure and business practices are properly reflected in the policy.

4.1.2. Updates to the policy and the supporting policies, standards and guidelines will be made periodically and will be announced by email broadcast or through other agency's established official communication channels

4.1.3. The most up to date approved version of this policy is kept within the agency's administrative registry.

4.2. Policy Distribution & Awareness

4.2.1. Hard copies of the policy and its supporting policies, standards and guidelines will be available on request from the administrative registry of the agency.

4.2.2. The ICT Unit may make periodic policy announcements by email or through other agency established official communication channels.

4.2.3. PO-RAMD heads of departments and units will ensure that all existing and new staff, contractors, subcontractors, and third party commercial service providers who report to them are made aware of and have access to the policy and its supporting policies, standards and guidelines.

4.2.4. Individuals requiring clarification on any aspect of the policy and its supporting policies, standards and guidelines and/or advice on general ICT Security matters may do so by contacting the ICT Unit.

4.3. Breaches of Security

4.3.1. For security and technical reasons PO-RAMD reserves the right to monitor, record and log all use of its Information and Communication Technology resources and activity on PO-RAMD network.

4.3.1. Any individual suspecting that there has been, or is likely to be a breach of ICT Security must inform their superiors, and the ICT Unit immediately. The ICT Unit will then advise the administration section on what action should be taken.

4.3.2. PO-RAMD reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. PO-RAMD staff, contractors, sub-contractors or authorized third party commercial service providers that use the agency's ICT resources and/or process information on behalf of PO-RAMD who breach this policy may be subject to disciplinary action, including suspension and dismissal as provided for in PO-RAMD disciplinary procedures or as prescribed in e-Government Act 2019.

4.3.1. Exceptions

In case of any exceptions to this policy, it shall be thoroughly documented and follow through a proper channel of authorization using the same authority which approved this document.

4.4. Roles and Responsibilities

4.4.1. Director of Records and Archives Management Department:

4.4.1.1. Shall be the overall Authority for the ICT Security Management of PO-RAMD ;

4.4.1.2 Shall be the appointing authority of the Department's Single Point of Contact for ICT Security.

4.4.2. ICT Security Single Point of Contact

4.4.2.1. Shall advise on the development of ICT Security Strategic Plan or incorporate ICT Strategic Issues as part of ICT Strategy and / or Corporate Strategy for the PO-RAMD ;

4.4.2.2. Shall identify current and future ICT Security technology needs for the PO-RAMD ;

4.4.2.3. Shall monitor and evaluate ICT Security Achievements against ICT Security Strategic Plan, ICT Strategic Plan, and / or Corporate Strategic Plan;

4.4.2.4. Shall provide advice and recommendations to ICT steering committee on pressing ICT Security Matters affecting PO-RAMD.

4.4.3. Directors/Head of Sections/Units

4.4.3.1. Shall be responsible for implementation of ICT Security plans falling under areas of their responsibilities through coordination and liaising with ICT Security Single Point of Contact.

4.4.3.2. Shall supervise all ICT Security issues falling under their areas of responsibilities for execution.

4.4.4. Employees

4.4.4.1. All employees of PO-RAMD shall have basic ICT security awareness training, any suspicious issue related to ICT security shall be reported to the relevant authorities.

4.4.4.2. Complying with the terms of this policy and all other relevant PO-RAMD policies, procedures, regulations and applicable legislation;

4.4.4.3. Respecting and protecting the privacy and confidentiality of the information they process at all times;

4.4.4.4. Complying with instructions issued by the ICT Unit on behalf of PO-RAMD ;

4.4.4.5. Reporting all misuse and breaches of this policy to their respective supervisors immediately;

4.4.4.6. Reporting all actual or suspected breaches of data security to their supervisors, PO-RAMD's administrative section and the ICT Unit immediately.

4.4.5. Internal Audit

Internal Audit are responsible for:

Providing assurance that Information and Communication Technology controls and procedures are operated in accordance with the policies, regulations and best practice.

SECTION FIVE

REFERENCE DOCUMENTS

5.1. ICT Policy

5.2. ICT Strategy

5.3. Acceptable ICT Use Policy

5.4. Other ICT Management Documents

SECTION SIX

DOCUMENT CONTROL

VERSION	NAME	COMMENT	DATE
Ver. 0.001	ICT Security Policy	Approved Draft	December, 2020