
BANK OF TANZANIA

# INFORMATION SECURITY GUIDELINES

TABLE OF CONTENTS

# DOCUMENT CONTROL

## Authors

| Name | Date |
|---|---|
| James Masoy, Maureen Mbowe, Frank Shayo, Michael Mtweve, Gati Michael, Francis Phillipo, Medard Charles, Calister Simba | 28/02/2022 |

## Reviewers

| Name | Date |
|---|---|
| Joel Ngussa, Flora Mwaigomole, Simon Sakilu | 01/04/2022 |

## Approval

| Name | Date |
|---|---|
| ICT Steering Committee | 24/06/2022 |

## Distribution

| Recipient | Title/Function | Date |
|---|---|---|
| Management | Heads of Directorates and Independent Departments | 024/06/2022 |
| All employees | Bank Employees | 24/06/2022 |

Amendment History

| Version | Date | Amendment Description |
|---|---|---|
| 1.0 | 01/09/2015 | Approved by the Management Committee |
| 1.1 | 23/03/2022 | Reviewed by authors |
| 1.2 | 01/04/2022 | Reviewed by Technical and Management Committee |
| 2.0 | 24/06/2022 | Approved by the ICT Steering Committee |

## Consultation

All comments regarding this document should be forwarded to Head of Information System Services.

## ABBREVIATIONS

| Abbreviation | Meaning |
|---|---|
| CA | Certificate Authority |
| CRL | Certificate Revocation List |
| DHCP | Dynamic Host Configuration Protocol |
| DMIS | Director, Management Information Systems |
| DMZ | Demilitarized Zone |
| DNS | Domain Name Server |
| ICT | Information and Communication Technologies |
| ID | Identification |
| IT | Information Technology |
| PKI | Public key Infrastructure |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| TLS | Transport Layer Security |
| TZ-CERT | Tanzania Computer Emergency response Team |
| WLAN | Wireless Local Area Network |

# GLOSSARY OF TERMS

| Term | Definition |
|---|---|
| Access | Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. |
| Access Rights | Authorized entry into a computer system to read, write, modify, delete or retrieve information contained therein. |
| Administrator account | A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. |
| Antimalware | is a software that protects a computer, system or an entire network from malicious infections that can be caused by a variety of malware. Types of malware includes viruses, computer worms, ransomware. |
| Application | A software program that is designed to perform a defined business function. |
| Asset Inventory | Register of assets |
| Asymmetric encryption | A cryptographic algorithm that uses two related keys, a public key and a private key. |
| Audit Trail | A record showing who has accessed an information system and the activities that have been performed during a given period. |
| Authentication | Verifying the identity of a user, process, or device to allow access to resources in an information system. |
| Authentication Credential | Evidence presented by the user, process, or device during verification process to gain access to an information system. |
| Authentication Mechanism | Hardware or software-based method that forces users, devices, or processes to prove their identity before accessing data on an information system. |
| Blog | Discussion published on the website consisting of posts that are regularly updated and typically displayed in reverse chronological order |
| Certificate Authority (CA) | A trusted entity that issues digital certificates and verifies the identity of the holder of the digital certificate |

| Term | Definition |
|---|---|
| Certificate Revocation List (CRL) | A list of revoked public key certificates created and digitally signed by a Certification Authority |
| Computer Room | A space (often designed with additional/backup power and cooling supply and protective systems) that houses computer servers, and communications equipment. |
| Data Center | A space (often designed with additional/backup power and cooling supply and protective systems) that houses computer servers, storage systems and communications equipment. |
| Database | A collection of information arranged in a structured format. |
| Database Administration | The role generally associated with the management and control of a Database. |
| Demilitarized Zone | Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks |
| Digital certificate | A set of data that uniquely identifies a key pair (Private and Public Keys) and an owner that is authorized to use the key pair. |
| Disclaimer | A statement appended to the end of an outgoing email reiterating the fact that the article reflects its author's opinion and not necessarily those of the organizations running the computer through which the article entered the network. |
| Dual connection | Client device that is connected to both a wired network and a WLAN at the same time |
| E- mail | A system for sending and receiving messages electronically over a computer network. |
| Emergency change | A Change that must be introduced as soon as possible |
| Encryption | The process of changing plain text into cipher text (encoded text) for the purpose of security or privacy. |
| Encryption Algorithm | Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key |

| Term | Definition |
|---|---|
| Endpoints Devices | Refers to end-user machines such as desktop computers, laptops, ipads and smartphones |
| Extranet | A private network that uses Web technology, permitting the sharing of portions of enterprise information or operations with suppliers, vendors, partners, customers, or other enterprises. |
| Firewall | A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures |
| Hardware Token | Smart card, metal key, or other physical object used to authenticate identity |
| Help desk | A service providing information and support to computer users. |
| ICT Equipment | Tangible IT assets, such as computer hardware and network or communication devices. |
| Information Asset | Knowledge or data that has value to the Bank |
| Information System | Discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information |
| Internet | It is a single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB), and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN). |
| Intranet | Bank Internal Computer Network (including, internal website, servers, and computers) that facilitate communication and collaboration within an organization with excluded access to external users. |
| Log | A record of events occurring within information systems. |
| Malware | A program with the intent of compromising the confidentiality, integrity, or availability of data or information system. |
| Multi-factor Authentication | Authentication using two or more different factors to achieve authentication. The factors may include something the user knows (e.g., PIN, password); something a user has (e.g., cryptographic identification device, token); or something the use is (e.g., biometric) |

| Term | Definition |
|---|---|
| Non-Disclosure Agreement | An agreement that outlines specific information, materials, or knowledge that the signatories agree not to release or divulge to any other parties |
| Non-repudiation | Protection against an individual falsely denying having performed a particular action. |
| Password | A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources.<br>This also include Personal Identification Number (PIN) which means an alphanumeric code or password used to authenticate an identity |
| Peer-to-peer | Relates to networks in which each computer can act as a server for the others, allowing shared access to files and peripherals without the need for a central server. |
| Private key | The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data. |
| Public key | The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. |
| Remote Access | The ability to access internal Bank network resources from other networks. |
| Security risk | Risk related to any event that compromises confidentiality, integrity and availability of information assets. |
| Social media | Interactive technologies and digital channels that facilitate the creation and sharing of information, ideas, interests, and other forms of expression through virtual communities and networks. |
| Spam emails | Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages |
| Standard user account or unprivileged user | Individual or system process authorized to access an information system with limited access rights. |
| Storage media | Device which is used to store data and information |
| Strong authentication | The requirement to use multiple factors for authentication and advanced technology, such as dynamic passwords or digital certificates, to verify an entity's identity. |

| Term | Definition |
|---|---|
| Subordinate CA | In a hierarchical PKI, a Certification Authority whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. |
| Symmetric Encryption | Encryption that uses the same secret key for encryption and decryption. |
| System account | The most privileged user such as root or administrator that has no restriction on the system. |
| Third Party | A person other than the Bank employee authorized by the Bank to provide or receive goods or services. |
| Transport Layer Security (TLS) | An authentication and security protocol widely implemented in browsers and Web servers |
| User | Individual or system process authorized to access an information system |
| User ID | Unique symbol or character string used by an information system to identify a specific user. |
| Virtual Meeting | A virtual meeting is a meeting held in a forum other than face to face usually using mobile or Internet connected devices |
| Wireless Local Area Networks (WLAN) | are groups of wireless networking nodes within a limited geographic area, such as an office building that are capable of radio communication which are usually implemented as extensions to existing wired local area networks (LAN) to provide enhanced user mobility and network access |

# 1. INTRODUCTION

The Bank maintains information assets to facilitate execution of its business operations. In recognizing the importance of the Information assets, the Bank has formulated Information Security Policy, 2021 to protect them. These guidelines aim at facilitating successful implementation of the policy.

# 2. OBJECTIVE

These guidelines provide guidance on protection of Bank's Information Assets in line with the Information Security Policy.

# 3. SCOPE

These guidelines shall apply to information systems which store, process, transmit or exchange Bank information assets.

# 4. ACCESS CONTROL

Access to information and information systems need to be controlled based on business and security requirements. Hence, this section outlines guidance for appropriate access controls to the Bank information assets.

## 4.1 Business Requirements for Access Control

(i) No person shall access any information asset unless authorized by responsible Head of Business Unit.

(ii) Access rights to the Bank's information systems shall be granted based on user's specific business needs and the need to maintain segregation of duties.

(iii) Access roles and corresponding privileges shall be established for each system to indicate various access profiles that can be assigned to users.

(iv) Suitable identification and authentication mechanisms shall be deployed to information systems to confirm legitimate users while considering sensitivity and security risk exposures.

(v) Information systems shall not allow multiple login sessions of the same username from multiple workstations.

## 4.2 User Access Management

### 4.2.1 User registration

(i) Access to information system shall be subject to user registration procedures.

(ii) Each user shall have user ID for access to information system.

(iii) Creation and use of generic user IDs is not allowed unless authorized by the Head Management Information Systems.

(iv) User access credentials shall not be used by any person other than the one assigned.

(v) Users are responsible for activity performed using assigned user IDs.

### 4.2.2 User De-activation and Activation

(i) Users shall be deactivated from accessing information system during unpaid leave, suspension, full-time training, or secondment without pay.

(ii) System administrators shall timely deactivate users absent from the office upon receiving notification from Head of Human resources and administrative function or authorization from respective Head of Information System function.

(iii) Retirees maintaining active account with the Bank shall be provided with access to the Retirees Portal that shall offer limited services regarding their accounts.

(iv) The requirements in 4.2.2(i) and 4.2.2(ii) shall not apply to Human Resource Management System, email systems, Staff Payment System or any other system as shall be determined by top management.

(v) System administrators shall ensure that information systems are configured to inactivate users who have not accessed the system for at least 30 consecutive days.

(vi) System administrators shall timely deactivate employees separated from the Bank upon receiving authorization from Head of Human Resource.

(vii) Activation of users shall require authorization from the head of business unit of the requesting user.

### 4.2.3 Maintenance and Review of User Access Rights

(i) Heads of business unit shall inform the Head Management Information Systems function to modify users' access rights to information system whenever there is a change of role.

(ii) IT Security administrators shall review user access rights for information systems on quarterly basis.

### 4.2.4 Handling of Administrator and System Accounts

(i) Head Management Information Systems shall ensure that system accounts are identified for each information system.

(ii) Authentication credentials for system accounts shall be managed according to the password guidelines.

(iii) System account shall only be used to perform system administrative activities.

## 4.3 Network Access Control

### 4.3.1 Intranet Access Control

(i) The Network administrator shall design and implement network controls such that the intranet is separated from other networks to protect the internal network resources and provide continuity of network services.

(ii) Employees or third parties shall not, unless authorized, access the internal network using private devices.

(iii) No user shall connect a computing device to the Bank network and any other network at the same time.

(iv) No third party shall access internal network unless authorized by the Head of Management Information Systems.

(v) System Administrator shall not allow use of insecure network protocols.

### 4.3.2 Extranet Access Control

(i) Where the Bank and other party intend to share business services through extranet, the responsible Head of business unit shall initiate a formal arrangement to be entered between the Bank and the other party.

(ii) The Network Administrator shall implement controls to logically separate various extranet domains based on requirements for business, security and terms defined in the formal arrangement.

(iii) Network administrator shall implement strong authentication and authorization mechanisms to prevent unauthorized access to network resources provided on the extranet.

(iv) Where there is a need to establish a site-to-site connectivity with a business partner, the Bank shall require the business partner to provide an independent assurance report indicating adequacy of security controls of the application intending to interact with Bank application prior to establishment of such connectivity.

### 4.3.3 Wireless Access Control

(i) Bank Wireless Local Area Networks (WLAN) that facilitate access to Bank internal resources shall only be accessible using pre-registered endpoint devices.

(ii) Bank WLANs shall only provide network services approved by the Head of Management Information System based on business needs.

(iii) Bank WLAN facilities located in publicly accessible rooms (such as Bank Conference Centers) which are intended to provide Internet services to non-employees shall be separated from the Bank Internal Network.

(iv) Employees and third parties are not allowed to connect personal wireless devices (such as Wireless Access Point) or any device that provides network services (such as DNS, DHCP) on the Internal Bank network.

(v) Network Administrator shall ensure that Bank network devices delivering wireless network services are securely configured.

### 4.3.4 Remote Access Control

(i) No person shall be allowed to access the internal network from external networks unless authorized by Head of Management Information Systems.

(ii) Remote access users shall be limited to specific network resources as approved by the Head of Management Information Systems.

(iii) Network Administrators shall ensure that any remote access to internal networks is encrypted using strong encryption algorithms.

(iv) Network Administrators shall ensure that any remote access to internal networks uses strong authentication mechanism.

(v) Devices used for remote access shall be required to have adequate security controls such as latest security patches, updated antivirus software and personal firewall.

(vi) Once remote access session has been established, remote access server shall be configured to disconnect the remote device from accessing any other networks.

### 4.3.5 Internet Access Control

(i) Network Administrators shall implement security mechanisms to facilitate timely detection and response to network attacks.

(ii) Network Administrators shall implement controls to filter network traffic entering or leaving the Bank network.

(iii) The Bank Internet connectivity shall be designed and implemented to provide resilient Internet Services that meet business requirements for Recovery Point Objective (RPO).

## 4.4 Operating System Access Control

(i) System Administrator shall ensure that operating systems are properly installed, configured, and maintained in line with configuration management standards. The configuration management standard at minimum shall require system administrators to change default settings, activate event logging and disabling insecure services.

(ii) Users shall be granted with access rights sufficient to perform assigned duties.

(iii) System administrators shall ensure that operating system security patches are timely applied.

(iv) System administrator shall ensure that operating systems are maintained with updated anti-malware.

## 4.5 Database Access Control

(i) Database Administrator shall ensure that databases are properly installed, configured, and maintained in line with configuration management standards. The configuration management standard at minimum shall require system administrators to change default settings, activate event

logging, setting of appropriate user access roles and disabling insecure services.

(ii) Database Administrators shall expire all default database accounts that are not needed for day-to-day database operations.

(iii) Default database accounts that are needed for routine database operations shall be set with strong passwords and controlled in accordance to Bank Password Management guidelines.

(iv) Live data shall not be used for training, presentation, or development purposes unless such data have been sanitized to conceal its sensitivity and confidentiality.

(v) Database Production environment shall not be used for testing purposes.

(vi) Database Administrators shall establish, implement, and regularly test an appropriate backup strategy for each database considering business requirements for Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

(vii) Database Administrator shall implement appropriate auditing of user activities and securely maintain database audit trail for review.

(viii) No change shall be applied into a production database unless authorized and tested.

(ix) Database Administrator shall ensure that security patches and updates are timely applied.

## 4.6 Application Access Control

(i) Applications shall have multiple controls at various stages of data input, processing, and output to protect the application from attacks.

(ii) Application shall have capability for enforcing segregation of duties and accountability among users.

(iii) Application shall have capability for enforcing strong authentication mechanisms such as use of multi-factor authentication.

(iv) Applications shall enforce creation of strong passwords in conformance to Bank's Password Management guidelines.

(v) Applications shall not be configured to transfer data across the network in clear text form.

(vi) Applications shall be capable of managing user privileges based on their roles and responsibilities.

(vii) Application Administrator shall securely keep documentation for applications.

(viii) No change on application shall be applied into a production unless tested and authorized.

## 4.7 Physical Access to Data Center and Computer Rooms

(i) Physical access to areas where information systems are deployed shall be restricted to authorized individual.

(ii) Entries to areas where information systems are stored shall be controlled by use of a combination of strong authentication mechanisms such as access control card, PIN, or biometric controls.

(iii) Audit trails for individuals gaining physical access to information systems areas shall be securely maintained.

(iv) Visitors and third parties shall be supervised and be granted access for specific and authorized purposes

(v) Access rights to secure areas shall be regularly reviewed, updated, and revoked when necessary

(vi) Head Network and Office Automation shall authorize granting of access to data centers or computer room premises.

(vii) Head Internal Security or Branch Security Officer shall ensure monitoring of access to information System premises.

(viii) Head Internal Security shall put in place controls for restricting visitors and third party from accessing data center or computer room premises.

## 4.8 Protection of Endpoint Devices

(i) Endpoint devices shall not be connected on Bank internal network without authorization.

(ii) Employees are responsible to protect Bank information stored on endpoint devices.

(iii) Employees shall timely report to the Bank through helpdesk in the event of stolen or lost endpoint device that contains Bank information

(iv) Endpoint devices shall be installed with antimalware protection that shall regularly be updated.

(v) Employees or third party are responsible to timely apply security patches on endpoint devices used to process or access the Bank internal network resources.

(vi) Endpoint devices used by third party to access the Internet only especially using guest WLAN shall not be subjected to authorization.

## 5. PROTECTION OF INFORMATION ASSETS

Information assets play a significant role in executing Bank business operations, thus, underscores the importance of protecting such assets. This section outlines guidance for adequate protection of information assets.

### 5.1 Ownership and Inventory of Information Assets

(i) Head Management Information Systems shall establish and maintain inventory of information systems at the Bank.

(ii) Respective business unit creating information asset within the bank shall be the owner.

### 5.2 Handling and Disposal of Storage Media

(i) Storage media containing information asset shall be securely stored to avoid damage and unauthorized access.

(ii) The Head Management Information Systems shall identify and dispose storage media containing information asset without compromising its confidentiality.

### 5.3 Information Classification

(i) Head of Business Units shall classify information according to its value, legal requirements, sensitivity, and criticality to the Bank in line with Record Management Policy.

(ii) Information shall be provided with adequate level of protection considering its confidentiality, integrity, and availability.

(iii) Head of Business Units shall review classification of information assets whenever need arises.

### 5.4 Exchange of Information

(i) Employees shall be responsible for protection of the information transferred, shared, or exchanged with internal and external entities in line with business requirements, applicable guidelines, and regulations.

(ii) Employees shall exchange Bank information through secure channels.

## 6. ACCEPTABLE USE OF EMAIL, INTRANET, INTERNET, IT CONFERENCE FACILITIES AND SOCIAL MEDIA

Bank electronic communication facilities such as email, intranet, and Internet play vital role in delivering Bank services. Thus, the Bank is necessitated to establish acceptable use of guidelines to protect these facilities from internal and external threats.

### 6.1 E-Mail Usage

#### 6.1.1 E-mail Addresses

(i) Employee shall be assigned with a unique email address to facilitate work-related communication.

(ii) The Bank shall terminate the use of email address where the employee separates from the Bank.

(iii) Users shall refrain from replying to spam emails. Such email shall be deleted from user mailboxes.

#### 6.1.2 Email Communication

(i) Email shall not be used for creation or transmission of any offensive, obscene, indecent, fraudulent content or other material that may be considered immoral.

(ii) Use of private email for work related correspondence is not allowed.

(iii) Sending, forwarding, and replying of emails to a large group of recipients, is prohibited. In scenarios whereby a need arise, proper authorization should be obtained from respective head of unit.

(iv) Sending, forwarding, and replying to chain emails is prohibited.

(v) Any suspicious emails originating from trusted or untrusted sources should not be opened and should be reported to Helpdesk.

(vi) Employee shall refrain from sending emails with large attachments. Size of email attachments shall be limited to 10MB. Where necessary, employee is encouraged to use authorized shared drives available on the internal network.

(vii) Employee shall exercise caution when giving out their email addresses to external parties to reduce the risk of Bank users becoming target of mail attacks.

(viii) Email transmitted to external recipients shall bear a short-form disclaimer to avoid potential legal consequences. A detailed form disclaimer shall be published on the Bank's public website. The short form and detail form disclaimers is presented in appendix 1.

### 6.1.3 E-mail Security

(i) E-mail passwords shall be maintained in accordance with the Bank Password Management guidelines.

(ii) Employee is accountable for misuse of email account.

(iii) Unauthorized access to other employees' emails is prohibited.

(iv) Unattended web email sessions for the duration exceeding three minutes shall be automatically logged off to prevent unauthorized use.

(v) Head Network and Office Automation shall ensure availability and timely update of anti-malware software.

(vi) System administrator shall ensure communication channels between email user and the server are encrypted.

(vii) All outgoing and incoming emails shall be automatically scanned for malicious content. Emails containing harmful content shall be cleaned, rejected, or blocked.

(viii) Confidential information sent via emails to external recipients shall be secured through encryption.

### 6.1.4 Managing E-mail Records

(i) E-mails shall be centrally retained and archived by System Administrators for recovery and future reference.

(ii) System administrators shall set storage limit per email user address.

## 6.2 Internet usage

### 6.2.1 Personal use of the Internet

The Bank's internet service is to be used for the sole purpose of facilitating business operations. It shall not be used for any other purpose.

### 6.2.2 Compliance to license and copyright requirements

(i) Users shall not download any content found on the Internet without establishing whether such action would be in violation of laws including but not limited to Intellectual Property laws.

(ii) Users are prohibited to download or install unlicensed software on computer devices connected to the Bank's network.

(iii) Users shall not access or subscribe to Internet sites that may in any way damage the reputation of the Bank or cause liability to the Bank by violating any law.

### 6.2.3 Protection of Bank's internal network

(i) Use of portable storage devices such as flash drive, memory cards, Compact Disks and external hard drives is prohibited unless authorized by the Head Management Information Systems.

(ii) Authorized users shall be responsible for scanning their portable storage devices when used on Bank computer devices.

(iii) Installation of unauthorized software to Bank computer devices is not allowed.

(iv) Content sent or received through Bank internet service shall be filtered to protect internal network against attacks.

(v) Users shall not access or subscribe to Internet sites containing pornographic, obscene, and immoral or any other inappropriate content.

### 6.2.4 Social Media

(i) The Head Public Relations and Protocol shall be responsible for disseminating Banks' information through social media in line with established procedures.

(ii) Private use of social media by employees shall be in line with the Bank Communication Strategy.

### 6.2.5 Preserving Internet bandwidth

(i) Use of Internet telecommunication facilities such as video conferencing and streaming for purposes not related to Bank operations is not allowed.

(ii) Users shall not access or subscribe to any internet services that are not related to assigned duties at the Bank such as music streaming, video broadcasting and Internet radio broadcast.

(iii) Use of peer-to-peer software on computer devices connected to the Bank network is not allowed.

(iv) Users are discouraged to download or upload big sized files that impede performance of Bank internet services.

### 6.2.6 Monitoring Internet Usage

(i) Users shall be aware that Internet utilization is recorded.

(ii) The Bank reserves the right to inspect, monitor, filter and disclose the contents of any Internet utilization through the Bank's computer networks or Internet system.

## 6.3 Intranet Access

### 6.3.1 Use of Intranet

(i) Users shall not disseminate to unintended recipient any information obtained from the Bank Intranet as such information may be confidential.

(ii) Third parties are not allowed to access the Intranet unless authorized by the Head of Management Information Systems; such access shall be restricted to the information requested.

(iii) Users of the internal Bank Blog shall not use the service in a manner that compromises security of Bank Information or violates existing laws, policies and guidelines.

### 6.4 Publishing on the Internal and Public Websites

(i) No contents shall be published on the internet websites without the permission of the Head Public Relations and Protocol.

(ii) The Head of Business Units shall be responsible to publish contents for their respective Business Unit on the Bank intranet.

### 6.5 Use of Information Technology Conference Facilities

(i) Organization of virtual meetings shall be carefully arranged to involve only eligible participants.

(ii) Employees are required to observe sensitivity of information shared through IT conference facilities and appropriateness of surrounding environment.

(iii) Security features built in IT conference facilities shall be utilized to ensure safe participation in virtual meetings

## 7. PASSWORD MANAGEMENT

Password is one of the means used to restrict unauthorized access to Bank information systems. Hence, password must be properly managed during creation, maintenance and use to minimize possibilities of unauthorized access to Bank information systems.

### 7.1 Password Requirements

(i) Password length shall be at least eight characters that contain upper and lower case characters (e.g., A-Z, a-z), digits (0-9) and special characters (e.g. @, #,*, $).

(ii) Users shall not reuse their passwords until 180 days have elapsed or after six cycles of password change.

(iii) Password shall not be similar to a user id or contain employee common details

(iv) User is not allowed to share password.

## 7.2 Changing Passwords

(i) New system users shall be supplied with initial passwords which they will be forced to change during initial login.

(ii) Users should be able to reset their passwords by using self-service mechanism provided by the system.

(iii) User shall change password after every 30 days or whenever there is a suspected security breach.

(iv) System Administrator shall change password after every 30 days or whenever there is a suspected security breach.

## 7.3 System Password Requirements

(i) Transmission of passwords between client and server shall be encrypted using strong encryption algorithm to avoid exposure of the password.

(ii) System shall have capabilities for administrator to reset user password.

(iii) System shall have capability for automatic locking of user ID after a maximum of three consecutive failed login attempts.

(iv) System shall store passwords in an irreversible encrypted form.

(v) Password shall not be displayed by the system in clear text.

(vi) System shall be configured to keep record of successful and failed login attempts.

(vii) System shall support creation of unique user ID linked to individuals and passwords to discourage use of generic users.

## 7.4 Protection of Administrative Passwords

(i) System administrators shall be required to change default passwords during deployment of newly acquired or upgraded systems.

(ii) Use of administrative accounts to perform non administrative operations is prohibited.

(iii) Direct access of system using system administrative accounts is prohibited.

(iv) System administrative Accounts such as root, administrator and schema accounts shall be changed after every 90 days or whenever there is a suspected security breach.

## 8. HANDLING THIRD PARTIES

The Bank engages third parties in carrying out some of its activities. Proper management of third parties facilitates information security. Hence, this section outlines guidelines to be observed during engagement with third parties to ensure protection of Bank information assets.

### 8.1 Information Security in Third Party Agreements

(i) The Head Management Information Systems shall-

(a) Maintain inventory of third parties allowed to access Bank information.

(b) Define levels of information access granted to different third parties, monitor and control the access to avoid exceeding agreed levels.

(ii) The Head of Business Unit shall consult other relevant business units including Head Management Information System while preparing information asset sharing agreement with third party.

(iii) Where a Third Party is an employee of the Government of Tanzania, such an employee shall be required to adhere to Bank Information Security policy including signing a Non-Disclosure Agreement or form.

### 8.2 Monitoring and Review of Third-Party Services

The Head Management Information System shall monitor and regularly review third party services to verify adherence to the agreements and take appropriate actions to resolve any identified problems.

### 8.3 Managing Changes to Third Party Services

The responsible Business Unit shall ensure that third parties do not effect any changes to the services provided without consulting the Head Management Information Systems and obtaining approval from the Accounting Officer.

## 9. MONITORING OF INFORMATION SECURITY

Information security monitoring is key in determining whether implemented controls are operating as intended and in providing compliance assurance. Various approaches are applied to assess effectiveness of information security controls and detection of security breaches. These include performing periodic technology

vulnerability assessments and penetration testing, reviewing of logs and timely reporting of security breaches.

This section provides guidance for assessing the effectiveness of implemented information security controls and applying appropriate corrective measures for continuous improvement.

## 9.1 Technology Vulnerability Management

(i) Head Network and Office Automation shall implement automated solutions to manage vulnerabilities of information systems.

(ii) Head Information Systems Services shall carry out or authorize vulnerability assessment on the information systems on a regular basis or as need arises, to identify weaknesses and propose appropriate measures.

(iii) Responsible Heads of Business Units shall implement measures proposed as an output of vulnerability assessment to address the identified vulnerabilities in line with change management procedures.

(iv) Employees familiar with vulnerabilities on Bank Information Systems shall report the weaknesses to IT Security Administrators through help desk.

(v) The results of vulnerability assessment on Bank Information Systems shall be confidentially maintained.

## 9.2 Penetration Testing of Information Systems

(i) Head Information Systems Services shall carry out penetration testing of information systems on a regular basis to identify weaknesses and propose appropriate measures.

(ii) The Head Management Information Systems shall process Management approval to engage government authority or any other authorized entity to perform penetration testing of Bank information systems.

(iii) Responsible Heads of Business Units shall implement measures proposed as an output of penetration testing in line with existing change management procedures.

(iv) Results of penetration testing on Bank Information Systems shall be confidentially maintained.

### 9.3 Collection and Review of Information System Logs

(i) Application, Database, System and Network Administrators shall configure information systems to record audit logs that are relevant to the information security monitoring process.

(ii) IT Security Administrators shall provide requirements for logging Information systems activities that are relevant for information security monitoring process.

(iii) IT Security Administrators shall review logs generated by Bank Information Systems to detect events related to system malfunctioning, performance, or security breaches on monthly basis

(iv) Information system logs shall be securely maintained to minimize the risk of unauthorized access or deletion.

### 9.4 Reporting Information Security Issues

(i) IT Security administrators shall regularly prepare and submit a report on information security monitoring with recommendations (if any) to the Head Management Information Systems for appropriate action.

(ii) The Head Management Information Systems shall submit to the ICT Steering Committee a consolidated report on information security issues and challenges for deliberation quarterly.

## 10. MANAGING INFORMATION TECHNOLOGY RISKS

(i) The Head Management Information Systems shall periodically perform risk assessment on IT systems and related infrastructure in line with the Corporate Risk Management Framework and Guidelines.

(ii) Responsible heads of business units shall implement risk mitigation measures within the recommended implementation timelines.

(iii) The Head Management Information systems shall maintain Information Technology risk register and status of implementation of mitigation measures

that shall annually or on demand be communicated to the Head Risk Management

## 11. OUTSOURCING OF INFORMATION TECHNOLOGY SERVICES

Where the Bank outsources any IT service, the management shall take appropriate measures to adequately manage the associated security risks. This section outlines guidelines for the protection of Bank's information assets involved in outsourced IT service environment.

### 11.1 Outsourcing Requirements

(i) Head Management Information Systems shall ensure that there is formal arrangement for outsourcing IT services.

(ii) During outsourcing of IT Services, the Head Management Information Systems shall consider the following:

(a) Ability of the Bank to oversee and control vendor managed processes

(b) Impact on data privacy and security

(c) The flexibility of the Bank to switch among available service providers when need arises

(d) Assurance on continuity of services by the provider

(iii) The Head Management Information Systems shall establish information security requirements for IT services to be outsourced.

(iv) The Head Management Information Systems shall ensure that there are arrangements for clear exit process and activities for both parties during termination.

### 11.2 Due Diligence

Where required to conduct due diligence of IT service provider, the Head Procurement Unit, shall consider adequacy of information security controls, business continuity and disaster recovery arrangements.

### 11.3 Managing Risks of Outsourced IT Services

(i) The Head Management Information Systems shall perform risk assessment of IT services to be outsourced that shall form the basis for deciding on outsourcing the services.

(ii) The Head Management Information Systems shall implement appropriate risk mitigation measures prior to outsourcing the IT service.

### 11.4 Service Level Agreement (SLA)

The Head Management Information Systems shall ensure that there shall be an SLA for each outsourced IT service. At minimum the SLA shall provide for -

(a) Objective and scope of outsourced services.

(b) Responsibilities of the parties.

(c) Metrics for assessing performance of the service provider.

(d) Notification procedures for handling incidents and related matters.

### 11.5 Review and Monitoring of Outsourced IT Services

(i) The Head Internal Audit shall provide reasonable assurance on risk management measures taken for respective outsourced IT services.

(ii) The Head Management Information Systems shall regularly review and monitor the outsourced IT services to ensure that Bank expectations are achieved as stipulated in the terms of engagement.

## 12. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

Security is an essential aspect that needs to be integrated during design and implementation of information systems supporting the business processes. This section outlines guidelines for managing security during information systems acquisition development and maintenance.

### 12.1 Security Requirements and Testing

(i) Business requirements for new information systems, or enhancements to existing information systems shall include requirements for security controls.

(ii) Security of new or enhanced systems shall be reviewed and tested prior to those systems being deployed into production environment.

### 12.2 Protection of System Files and Application Source Codes

(i) Access to system files and application source code shall be controlled using centralized automated enterprise solution to avoid their exposure which can result to security breaches.

## 13. PROTECTION OF ENVIRONMENT FOR DATA CENTERS AND COMPUTER ROOMS

Information systems need to be kept in a well-controlled environment. Environmental controls include deployment of air conditioning system, fire suppression systems, smoke detectors and humidifiers. This section outlines guidelines for protecting the environment within which Bank information systems are kept.

(i) Head Estate Management or Finance and Administration shall allocate space suitable for Data center or computer room operations that is protected against natural and artificial hazards.

(ii) Head Estate Management or Finance and Administration shall install and maintain fire detection and suppression systems for securing data center or computer room premises.

(iii) Head Estate Management or Finance and Administration shall ensure that the premises for information systems have reliable power supply and cooling systems.

(iv) Power and data network cables shall be protected from interception, interference or damage.

## 14. INFORMATION SECURITY INCIDENT MANAGEMENT

Bank Information systems may be subjected to incidents which may affect information security and subsequently impair ability of the Bank to carry out its operations. Information security incidents or events may include loss of service equipment or facilities, attack executed via an email message or attachment, non-compliances with policies or guidelines, malfunctions of software or breaches of physical security arrangements.

This section outlines guidelines for handling information security incidents so as to minimize their impact on Bank operations.

## 14.1 Detection and Reporting of Information Security Incidents

(i) IT Security Administrators shall use automated security tools such as firewall, antimalware, and log monitoring to detect information security incidents

(ii) Employee or third party shall report information security incident to the IT Security Administrator through helpdesk for appropriate action.

## 14.2 Analysis and Containment of Information Security Incidents

(i) IT Security Administrator shall analyze and provide report on information security incidents and status of the resolution to the Head Management Information System for further action.

(ii) Where necessary, the Head Management Information Systems shall formulate a team that shall be responsible for handling information security incidents with significant impact to the Bank.

(iii) Head Management Information System shall on quarterly basis report to the ICT Steering Committee information security incident with significant impact.

(iv) Reported incident shall be analyzed and facts collected shall be in line with existing laws.

(v) Findings from incident analysis or investigation shall be documented and maintained confidentially.

## 14.3 Contact with External Authorities

(i) The Head Management Information Systems shall be the focal point of contact for communication with the National Computer Emergency Response Team (TZ-CERT) or other government authorities on information security threats or incidents.

(ii) The Head Protocol and Public Communication shall be responsible to communicate any information security related information that is intended to be addressed to the media or public.

(iii) The Head Investigation function shall be the focal point of contact for communication with law enforcement agencies on information security incidents.

The Head Management Information Systems shall share appropriate knowledge regarding information security incidents with external institutions in line with existing arrangement.

## 15. MANAGEMENT OF PUBLIC KEY INFRASTRUCTURE (PKI)

The Bank uses PKI technology to provide assurance on confidentiality, integrity, nonrepudiation, and availability of its information assets. This section outlines guidelines on protection of IT infrastructure that support for generation, dissemination, use, storage, backup and archiving of cryptographic related information.

### 15.1 MANAGEMENT OF CERTIFICATE AUTHORITY

(i) Systems Administrators shall physically protect and securely configure servers used for Certificate Authority (CA) to minimize risks of unauthorized key generation or compromise of digital certificates generated and stored on it.

(ii) The Head Management Information System shall authorize installation and use of CA or related subordinate CAs.

(iii) The Bank shall only use encryption algorithms that are globally tested and have no security weaknesses.

(iv) The Head Information System Services shall authorize issuance of a digital certificate that is stored on hardware token.

### 15.2 PROTECTION OF KEYS

(i) Symmetric encryption keys shall be securely stored to avoid disclosure.

(ii) Private keys shall securely be made available to and used only by the intended user.

(iii) The private key shall be stored on a hardware token protected by a passphrase known only to the individual to whom the token is issued or stored on a protected computer hard drive.

(iv) A private key issued for use by application shall be stored on a server directory that has restricted access by other users to minimize misuse.

(v) Users shall request for revocation of a digital certificate in case of a suspected security breach.

(vi) A Certificate Revocation List (CRL) shall timely be made known to users to avoid trusting revoked digital certificates.

## 15.3 BACKUP, RECOVERY AND ARCHIVING OF CRYPTOGRAPHIC KEYS

(i) Private keys associated with digital certificates used for encryption shall be retained until it is no longer needed to decrypt the data or information encrypted by that key.

(ii) Private keys associated with digital certificates used for authentication purposes shall not be backed up or archived to avoid compromise of non-repudiation.

## 15.4 HARDWARE TOKEN STORAGE AND PROTECTION

(i) Unused hardware tokens shall be adequately protected against unauthorized physical access.

(ii) Users shall adequately protect hardware tokens storing digital certificates against unauthorized physical access.

(iii) Users shall not leave hardware tokens connected to the computer while not in use.

(iv) Hardware tokens containing digital certificates shall be protected with strong password or passphrases as per Bank password management guidelines.

(v) The loss or theft of hardware token shall be reported to the Head Information System Services through Helpdesk for immediate revocation of the contained digital certificate.

## 15.5 PROTECTION OF SERVERS OR APPLICATIONS USING KEYS

(i) Production servers or applications using Transport Layer Security (TLS) and that are accessed from within the Bank internal network shall use

digital certificates signed by the Bank CA or known trusted provider depending on its security sensitivity.

(ii) Use of self-signed digital certificates on production servers or applications is not allowed.

(iii) IT Security Administrator shall monitor the validity of digital certificates for following up their renewal before expiry.

(iv) Application Administrator shall monitor and timely renew digital certificates before expiry.

(v) Servers or applications using TLS that are accessed from outside the Bank network shall have digital certificates signed by a known trusted provider.

## 16. COMPLIANCE AND ENFORCEMENT

(i) Bank Employees and third parties shall comply with these guidelines.

(ii) Appropriate action shall be taken against any employee or third party who fails to comply with these guidelines.

## 17. ISSUANCE AND REVIEW

(i) These guidelines are issued by the ICT Steering Committee

(ii) The guidelines shall be reviewed at least once in three years and whenever need arises

Issued on the 24th day of June 2022.

Julian Banzi Raphael
Jul 22 2022 11:27 AM

.....

DocuSign

Julian B. Raphael

**Chairperson ICT Steering Committee**

## Appendix 1

**Short form Disclaimer:**

*---------- ----------*

*---------- ----------*

*Disclaimer*

*---------- ----------*

*Nothing contained in this e-mail, that is, its main text and the attachments thereto shall be construed as legally binding to the Bank of Tanzania. The Bank of Tanzania shall not be liable in any way whatsoever for any loss or damage resulting from opening of this e-mail, including the attachments thereto or the use of information contained therein. Please, refer to the full disclaimer found at http://www.bot.go.tz/emaildisclaimer.htm*

*---------- ----------*

**Detail form Disclaimer:**

*The Bank of Tanzania shall not be liable in anyway whatsoever for any loss or damage resulting from opening of this e-mail, including the attachments thereto or the use of information contained therein.*

*If you have received this message in error or in any way that it was not intended to reach you please notify the original sender immediately and destroy the original message. You are hereby notified that you must not disseminate, copy, use, distribute, publish or take any action in connection therewith, as the message might be containing information that is confidential and restricted, thus subject to legal restrictions and sanctions.*