አዋሽ ባንክ
AwashBank

Circular No. 36/2023

To: - All Chief Officers
- All D/Chief Officers
- All Directors and D/Directors
- All Regional Directors
- All Branch Managers

From: Chief Executive Officer

Date: April 11, 2023

Subject:- Information Systems Asset Management Policy

Please find enclosed herewith the Information Systems Asset Management Policy for your perusal and implementation.

Softcopy of the Information Systems Asset Management Policy shall be distributed through the Office of D/Chief, Strategy Innovation & Transformation Officer. The Policy shall be put in force effective immediately.

All recipients of this Circular shall, therefore, ensure that the Policy is thoroughly read, understood and properly implemented. Thank you.

Encl:- Information Systems Asset Management Policy

Tel.: +251-0115-57-00-65/66 Fax: -0115-57-01-26 |Email:tsehayf@awashbank.com

አዋሽ ባንክ
AwashBank
Nurturing Like the River

Awash Bank Information Security Policy

Section 1: Information Systems Asset Management Policy

April 2023

Information

Title	Code	Classification	Version	Status
Information Systems Asset Management Policy	AB_ISMS_ISATEP_DOC	Internal	1.0	

Revision History

Version	Author(s)	Issue Date	Changes
1.0	Awash Bank	April 26, 2023	First version

Review, Verification and Approval

Name	Job Title	Date	Signature

Distribution List

Copy#	Recipients	Location

Table of contents

1. TERMS AND DEFINITIONS 4
2. INTRODUCTION 6
3. PURPOSE 6
4. SCOPE OF APPLICABILITY 6
5. USERS 6
6. REFERENCE AND RELATED DOCUMENTS 6
7. ORGANIZATIONAL STRUCTURE, ROLES AND RESPONSIBILITIES 7
   - 7.1. Organizational Structure 7
   - 7.2. Roles and Responsibilities 8
8. INFORMATION SYSTEMS ASSET MANAGEMENT 9
   - 8.1. Policy Statement 9
   - 8.2. Policy Details 9
     - *8.2.1. Planning, acquisition, delivery of information asset* 9
     - *8.2.2. Inventory of Information and Other Associated Assets* 9
     - *8.2.3. Classification of Information* 11
     - *8.2.4. Labelling of Information* 11
     - *8.2.5. Acceptable Use of Assets and Other Associated Information Assets* 11
     - *8.2.6. Return of Assets* 12
     - *8.2.7. Management of Storage Media* 12
     - *8.2.7.1. Use of Storage Media* 12
     - *8.2.7.2. Disposal of Storage Media* 13
     - *8.2.7.3. Storage Media Transportation* 13
   - 8.3. Policy Implementation 14
   - 8.4. Policy Violation 14
   - 8.5. Policy Exception 14
   - 8.6. Policy Owner and Custodian 14
   - 8.7. Policy Access and Communication 14
9. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 16
10. POLICY REVISION, REPEAL, REPLACEMENT, AND EFFECTIVE DATE 18
    - 10.1. Revision of the Policy 18
    - 10.2. Repeal and Replacement 18
    - 10.3. Effective Date of the Policy 18

1. Terms and Definitions

Table 1 provides definitions of the common terms used in this document

Term	Definition
Accountability	A security principle indicating that individuals shall be able to be identified and to be held responsible for their actions.
Asset	Anything that has value to the organization (primary assets: information, business processes and activities; supporting assets: hardware, software, network, personnel, site, organization's structure).
Asset Owner	A person or group of people who have authority for specified information asset, responsible for making sure that information assets are properly classified, protected and accessed appropriately, as a result that the value of the asset is fully exploited. The Owner may change during the lifecycle of the asset.
Asset Custodian	A person or group of people that are designated or delegated by the asset owner, having responsibility for the implementation and maintenance of the confidentiality, availability and integrity of an information asset.
Availability	The state of an asset or a service of being accessible and usable upon demand by an authorized entity.
Business Owner	A person or group of people who have authority for specified information asset, responsible for making sure that information assets are properly classified, protected and accessed appropriately, as a result that the value of the asset is fully exploited. A person or group of business specialists, who need to document what the business services are, how they are delivered and what applications contribute to creating client value. Ensure that it has adequate security controls based on the classification and define risk appetite.
Confidentiality	An asset or a service is not made available or disclosed to unauthorized individuals, entities or processes.
Control	A means of managing risk, including policies, procedures, and guidelines which can be of administrative, technical, management or legal nature.
Guideline	A description that clarifies what shall be done and how, to achieve the objectives set out in policies.
Incident	An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Information Security	The preservation of confidentiality, integrity, and availability of information. Additionally, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
Integrity	Maintaining and assuring the accuracy and consistency of asset over its entire life-cycle.
Labelling	Affixing a physical or electronic label identifying the security category of a document, file or records series in order to alert those who handle it that it requires protection at the applicable level.
Policy	A plan of action to guide decisions and actions. The policy process includes the identification of different alternatives such as programs or spending priorities, and choosing among them on the basis of the impact they will have.
Record	Information created, received and maintained as evidence and as an asset.
Risk	A combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

Term	Definition
System	An equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, control, display, switching, interchange, transmission or reception of data and that includes computer software, firmware and hardware.

Table 1: Terms and Definitions

2. Introduction

Asset management is a core process of an organization. Managing assets means applying a systematic approach to maintaining their lifecycle in a way that optimizes value. This includes having a policy/process in place to develop, operate, maintain, upgrade and dispose of assets in the best possible way. Overall Asset management establishes the blue print to identify the rules of acceptable use and the rules for protection: what assets to protect, who protects them, and how much protection is adequate.

Asset management involves applying deliberate processes to the design, use and maintenance of physical and intangible assets so their value is maximized, from beginning to end.

3. Purpose

The main purpose of information systems asset management policy is to identify Awash Bank's organizational assets and define appropriate protection responsibilities, ensure that information receives an appropriate level of protection in accordance with its importance to the bank, and prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

4. Scope of Applicability

This policy document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all information systems and other information assets used within the ISMS scope.

5. Users

Users of this document are all employees of Awash Bank and relevant external parties.

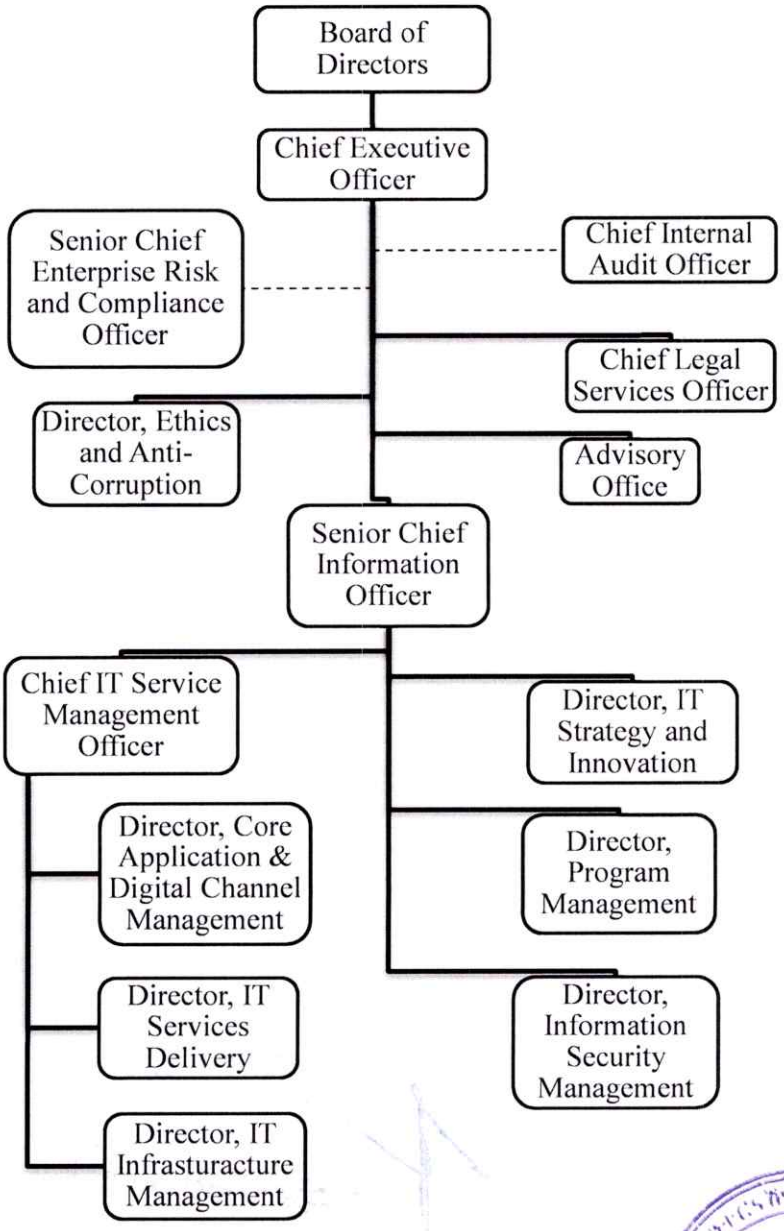
6. Reference and related documents

a. ISO/IEC 27001 Standard
b. INSA National Cyber Security Framework Development Methodology
c. Awash Bank Information Security Policy
d. Awash Bank Information Security Risk Management Policy
e. Awash Bank Information Classification Policy
f. Awash Bank Access Control Policy
g. Awash Bank Information Security Incident Management Policy
h. Awash Bank Acceptable Use Policy
i. Awash Bank Operations Security Policy
j. Awash Bank Supplier and Partner Relationships Security policy
k. Awash Bank Secure System and Software Acquisition, Development, and Maintenance Policy
l. Awash Bank Human Resource Security Policy
m. Awash Bank IT Service Management Policy

7. Organizational Structure, Roles and Responsibilities

The organization structure, roles and responsibilities of various organs of the Bank in relation to Information Systems Asset Management activities are indicated below.

7.1.Organizational Structure



7.2.Roles and Responsibilities

7.2.1 **Information Security Management Directorate** is responsible for:

a. Detecting and responding to information security violations, security breaches and vulnerabilities.
b. Monitoring compliance with information security polices and best practices.
c. Establishing policies and procedures that ensure protection of information assets.

7.2.2 **IT Infrastructure Management Directorate** is responsible for:

a. Maintaining and updating an asset inventory of Awash Bank's assets.
b. Managing and updating information assets of the bank.
c. Revoking access rights (logical and physical) to assets upon employee termination or change.

7.2.3 **HR Directorate, and other relevant unit** are responsible for ensuring resigned or terminated employee return all Awash bank's assets interested before they complete termination process.

7.2.4 **Information Security Steering Committee** is responsible for conducting and managing information security risk management activities.

7.2.5 **Asset Owner** is responsible for classifying the assets based on Information System Asset Management Policy and Procedure.

7.2.6 **Asset Custodian** is responsible for:

a. Implementing appropriate controls to protect the confidentiality, integrity, availability and authenticity of sensitive information.
b. Assigning value for the assets.
c. Applying security measures in protecting removable storage media.
d. Disposing unused information in a secure way.

7.2.7 **Business Owner** is responsible for assigning asset ownership for new assets in bank's environment.

7.2.8 **All user** is responsible:

a. To adhere to information security policies and procedures pertaining to the protection of information.
b. For reporting actual or suspected information security incidents to **Information Security Management Directorate**.

8. Information Systems Asset Management

8.1.Policy Statement

"Awash Bank acknowledges the need to manage its information assets throughout the lifecycle of the assets (i.e. planning, acquisition, delivery, deployment/installation, management, retirement and disposal). Therefore, the Bank is committed for the establishment of an effective information systems asset management policy/process/procedures for managing the critical asset of the Bank."

8.2.Policy Details

8.2.1. Planning, acquisition, delivery of information asset

8.2.1.1.The **Information Security Management Directorate** is responsible to ensure all security requirements are included during asset planning stage.

8.2.1.2.Any asset acquisition shall consider information security requirements as mandatory. The **Information Security Management Directorate** is responsible to provide detail information security requirements.

8.2.1.3.During the delivery of asset the **Information Security Management Directorate** shall ensure that security requirements are met within the asset acquisition stage.

8.2.1.4.The Information Security Management Directorate shall ensure asset management lifecycle activities meet the security requirements of the Bank.

8.2.2. Inventory of Information and Other Associated Assets

8.2.2.1.The **Asset Owner** shall identify it's information and information systems assets and define appropriate protection responsibilities.

8.2.2.2.The **IT Infrastructure Management Directorate** shall establish a process and procedure for delivery, recording, maintaining, and updating inventory of information and information systems assets. This inventory shall be categorized according to their type and criticality.

8.2.2.3.Assets inventory shall contain asset identification, description, location, classification, value, label, asset owner and asset custodian.

8.2.2.4.Assets depending on the sensitivity and criticality of its impact if exposed shall be classified as defined in the "Awash Bank Information Classification Policy".

8.2.2.5.The **Information Security Management Directorate** shall maintain and verify it's asset inventories on a regular basis and shall validate the measures taken to protect the assets as part of the bank's information security risk management activities.

8.2.2.6.The loss, theft, or misappropriation of assets shall be reported immediately to immediate supervisor and Information Security Management Directorate.

8.2.2.7.The **Business Owner** shall assign an asset owner for each assets. And shall designate asset custodians for assets, with approved management responsibility, for the protection of the bank's assets associated with information and technology systems or services.

8.2.2.8.All information and assets associated with information processing facilities shall be owned by a designated part of the Bank.

8.2.2.9. The bank shall ensure that there will be rules defined for the acceptable level of use for all the information assets of the bank

8.2.2.10. The bank shall ensure that all employee and external party users shall return all the bank assets in their possession upon termination of their employment, contract, or agreement.

8.2.2.11. The bank shall ensure all data and software shall be erased from equipment or asset prior to disposal or redeployment.

8.2.2.12. For each asset of the Bank, the following roles and responsibilities shall be applied:

Role	Responsibilities
Asset Owner	• Classifying the assets. • Defining the access rights of assets entrusted by the Bank's Management. • Ensuring that proper labeling whenever is applicable for sensitive information. • Ensuring that proper controls are in place to address confidentiality, integrity and availability of information. • Reviewing assets classification periodically. • Communicating security controls and protection requirements to the information custodian and user. • Defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies. • Defining and periodically reviewing backup schedules, restoration schedules, test results of backup and restorations and integrity of the data after restoration.
Asset Custodian	• Protecting bank's information to ensure its confidentiality, integrity and availability. • Applying information security policies and best practices to the information. • Determining and documenting the requirements for authorized access to the information. • Performing regular backup and data validity testing activities. • Reporting any suspected or actual security violations, security breaches, and incidences of compromised information to the asset owner. • Taking prior approval of the asset owner before sharing information. • Ensuring availability of information at all times and circumstances. • Performing control implementation and regular administrative tasks.
User	• Understanding the information asset classifications, abiding by the security controls defined by the asset owner and applied by the asset custodian. • Maintaining and conserving the asset classification and labeling established by the asset owner. • Contacting the asset custodian when information is unmarked or the classification is unknown. • Using the information only for approved purposes. • Reporting any suspected or actual security violations, security breaches, and incidents of compromised information to the Information Security Management Directorate.

8.2.3. Classification of Information

8.2.3.1. Information Classification shall be based on "Awash Bank Information Classification Policy".

8.2.3.2. The Information classifications shall always be based on the sensitivity, criticality, confidentiality, privacy requirements and value of the information.

8.2.3.3. All bank's personnel shall comply with the defined information classification scheme.

8.2.3.4. Results of information classification shall be updated in accordance with changes of their value, sensitivity and criticality through their life cycle.

8.2.3.5. If classified information is received from outside the bank, the **CEO** shall be responsible for its classification in accordance with the rules prescribed in Awash Bank Information Classification Policy, and **Information Owner / Asset Owner** becomes the owner of such an information asset.

8.2.4. Labelling of Information

8.2.4.1. **Asset Owner** shall be responsible for labelling the asset and maintaining the asset record. Labelling process shall be in accordance with approved Awash Bank's naming practices.

8.2.4.2. Assets shall be maintained, handled, stored, transported (or transmitted) and destroyed in accordance with the Information Labelling and Handling Guidelines associated with the asset's classification label.

8.2.4.3. The Bank shall define and establish procedures for handling and storage of information in order to protect such information from unauthorized disclosure or misuse.

8.2.4.4. Documents, hardware items and removable media physical labelling shall include appropriate security classifications in accordance with this Information Systems Asset Management Policy.

8.2.4.5. Media containing classified information shall not be handed over to any external entity or third party unless authorized by the bank with a proper business justification. The third part shall sign a Non-Disclosure Agreement (in case if media is damaged and it needs to return back to the third party).

8.2.4.6. Confidentiality level shall be labeled in accordance with the rules defined in Awash Bank Information Classification Policy.

8.2.5. Acceptable Use of Assets and Other Associated Information Assets

8.2.5.1. The Bank shall define an "Acceptable Use Policy" that provides guidelines for information systems asset management.

8.2.5.2. All the Bank's assets shall be used for business purpose only.

8.2.5.3. All the Bank's employees:

a. Shall acknowledge the need for protecting the Bank's information; and perform their daily activities in compliance with the information security policy.
b. Shall not participate in illegal activities such as unauthorized access of assets, hacking, introducing any computer contaminant or computer virus, committing acts which may disrupt use of the assets.

8.2.5.4. The Bank shall monitor, record, or periodically audit the use of any of its information, telecommunications systems and equipment. Actual or suspected misuse of these systems shall be reported to **Information Security Management Directorate** in a timely manner.

8.2.5.5. Awash Bank shall establish and define proper procedures for handling, processing, storing and communicating information based on its classification in order to protect this information from unauthorized disclosure or misuse.

8.2.5.6. Employees with custody of Awash Bank's sensitive information shall follow Awash Bank Access Control Policy to ensure that this information is protected from unauthorized access.

8.2.5.7. The use of storage media and peripheral devices (e.g., DVD writers, USB ports, flash disks, etc.) shall be limited for Awash Bank's business needs only. Centralized mechanisms that control and limit the use of such devices shall be considered.

8.2.5.8. Portable storage media holding unencrypted sensitive Awash Bank's information shall be placed in locked furniture when not in use.

8.2.5.9. Access to Awash Bank's sensitive information or valuable information shall be granted only to specific individuals, not groups, on a need-to-know basis and after Bank's Management authorization has been obtained.

8.2.5.10. Information assets shall be taken off-premises only after obtaining authorization.

8.2.5.11. All persons accessing classified information shall follow the rules listed in the Awash Bank Information Classification Policy.

8.2.6. Return of Assets

8.2.6.1. **HR Directorate**, and **other relevant directorates** shall ensure that the Bank's all employees return all assets (e.g., Laptops, Desktops, Printers, etc.) of the Bank in their possession upon termination of their employment, contract or agreement as per clearance procedure. This may include, but not be limited to:

a. A formal process for return (e.g., checklists against inventory) of the Bank's assets.
b. A formal process for return or destruction of the Bank's information of any kind.
c. Where employees use personal equipment, requirements for secure erasure of software and information belonging to the bank.

8.2.6.2. During the notice period of employee termination, the bank shall control unauthorized copying of any bank's relevant information such as software, business information and sensitive data.

8.2.7. Management of Storage Media

8.2.7.1. Use of Storage Media

8.2.7.1.1. Information security requirements shall be considered in the management of removable information and related technology media.

8.2.7.1.2. The following shall be considered for management of storage media:

a. Removable storage media drives shall be allowed if there is a business need.

b. All storage media shall be stored and kept in a safe, secure environment and in accordance with manufacturer's specifications and applicable Bank's information security policies and procedures.
c. Multiple copies of Awash Bank's valuable information shall be stored and kept on separate storage media to ensure its availability in case of data damage or loss.
d. In case of storage media is no longer require, its contents that need to be removed shall be made unrecoverable.

8.2.7.2. Disposal of Storage Media

8.2.7.2.1. All Awash Bank's sensitive storage media shall be disposed as per the "Information Systems Asset Management Policy and Procedure" retention period or end of use of storage media. Once storage media is disposed, it shall be documented and reported to the asset owner.

8.2.7.2.2. The asset owner's authorization shall be obtained before all storage media are removed or disposed.

8.2.7.2.3. All disposed storage media shall be logged in an updated storage media disposal log in order to maintain an audit trail.

8.2.7.2.4. All Awash Bank's sensitive information whether documented hardcopies or stored in electronic form that are no longer needed, shall be disposed in a secure way, using approved equipment and procedures to ensure that information cannot be recovered. Disposal shall be conducted using one of the following methods, but not be limited to:
a. Shredding.
b. Pulping / Recycling.
c. Incineration (i.e., converting it to carbon dioxide and waste vapor "Ash" by fire).

8.2.7.2.5. A record of disposed sensitive information shall be kept for at least **5 years** according to Bank's regulatory requirements. Record shall include as a minimum:
a. Date of disposal
b. The name of the person carrying out the disposal.
c. The name of the owner.
d. The obtained approval of the owner.
e. The disposal method followed.

8.2.7.2.6. Before storage media is sent to a third party, all Awash Bank's sensitive information shall be deleted, concealed, or replaced according to the Bank's approved methods.

8.2.7.3. Storage Media Transportation

8.2.7.3.1. Wherever possible, cryptographic techniques shall be used to protect the confidentiality, integrity and authenticity of sensitive information during physical media transportation.

8.2.7.3.2. All Awash Bank's sensitive information in hardcopy form shall be sent through a trusted courier or registered mail and shall always be tracked with a weigh bill

number and require recipient signature. Delivery of such information to intermediaries shall not be allowed.

8.3.Policy Implementation

8.3.1. When required, detailed procedure document shall be prepared to support the implementation of this policy.

8.4.Policy Violation

All employees of Awash Bank are required to ensure adherence to the highest level of professional ethics those are promulgated on the Bank's Information security policy standard and articulated herein. However, Non-compliance to the minimum requirements or violation of this policy may institute disciplinary action based on the respective Human Resource Policy and related Human Resource Security Policy that includes, but is not limited to, the following:

- Suspension;
- Termination;
- Civil and/or criminal prosecution;
- Other disciplinary action.
- Pursuing of an appropriate legal action under local, state or federal law.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

8.5.Policy Exception

8.5.1 Exceptional cases related to the service interruption should be approved by the CEO.
8.5.2 Exceptional cases related to emergency should be approved by the Senior CIO with the immediate reporting to the CEO.
8.5.3 All other exceptions, shall be approved by the Board of Directors (BoD).

8.6.Policy Owner and Custodian

8.6.1 The owner of this policy is the Bank.
8.6.2 The custodian of this policy shall be Information Security Steering Committee.

8.7.Policy Access and Communication

8.7.1 This policy document is internal document of the Bank and is meant for internal usage within the bank. Duplication and distribution of this policy without an authorized release is prohibited.
8.7.2 **Transformation & Change Management Directorate** shall decide on the number of copies that should be in circulation and the persons with whom the document should be available.

8.7.3 **Transformation & Change Management Directorate** has to ensure that all employees of Awash Bank and other relevant external parties are familiar with this policy.

8.7.4 **Information Security Management Directorate** is responsible for training and raising awareness of persons using this policy.

8.7.5 Every Person in custody of this document has the responsibility for ensuring its usage limited to "within Awash Bank". Any loss or mutilation of the document must be reported promptly to the **Information Security Management Directorate**.

9. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
List of Authorized persons with access to assets	Asset Owner computer / cabinet	Asset Owner	The same as for the protection of information	The list must exist as long as the information itself exists
Asset inventory/ Asset registry record	IT Infrastructure Management Directorate computer / cabinet	IT Infrastructure Management Directorate	Only IT Infrastructure Management Directorate can publish and edit Read access to other is in need-to-know basis only Malware protection	3 Years
Information Security Incident Response record	Information Security Management Directorate computer / cabinet	Information Security Management Directorate	Only Information Security Management Directorate can publish and edit. Read access to other is in need to know basis only	3 Years
Resigned or terminated employee clearance records	HR Operations Directorate computer/cabinet	HR Operations Directorate	Only HR Operations Directorate can publish and edit Read access to other is in need-to-know basis only Malware protection	Based on Human Resource Management Policy
NDA record for handling confidential information	Asset Owner computer/cabinet	Asset Owner	Only Asset Owner can publish and edit Read access to other is in need-to-know basis only Malware protection	Based on the agreement

Policy Violation Record	HR Operations Directorate computer/cabinet	HR Operations Directorate	Only HR Operations Directorate can publish and edit Read access to other is in need-to-know basis only Malware protection	5 year
Policy Exception Record	Asset Custodian's computer / cabinet	Asset Custodian	Only Asset Custodian can publish and edit Read access to other is in need-to-know basis only Malware protection	5 year

Only **Asset Custodian** can grant other employees access to any of the above mentioned documents.

10. Policy Revision, Repeal, Replacement, and Effective Date

10.1. Revision of the Policy

Unless there is a special enforcement to revise this Policy in the meantime, it shall be revised every three years and approved by the Board of Directors. The Information Security Steering Committee shall initiate and manage the revision of this Policy.

10.2. Repeal and Replacement

Any Information Security Policy of the Bank contravening this Policy, if any, are hereby repealed and replaced by this Policy.

10.3. Effective Date of the Policy

This Information Systems Asset Management Policy shall be in force effective from _____ 2023.

End of Document