አዋሽ ባንክ
AwashBank

Circular No. 49/2023

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 Classification Policy

Please find enclosed herewith the Information Classification Policy for your perusal and implementation.

Softcopy of the Information Classification 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 Classification 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 14: Information Classification Policy

April 2023

Information

Title	Code	Classification	Version	Status
Information Classification 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

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.

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

Protecting sensitive information of the bank such as client's data, employee's data and the likes are the paramount activities which are routinely practiced to prevent sensitive information of the bank fall into the wrong hands. So, it is crucial to the bank to ensure the security and integrity of information at all times.

3. Purpose

The purpose of information classification policy is to 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.

4. Scope of Applicability

This policy document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all types of information, regardless of the form – paper or electronic documents, applications and databases, etc.

5. Users

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

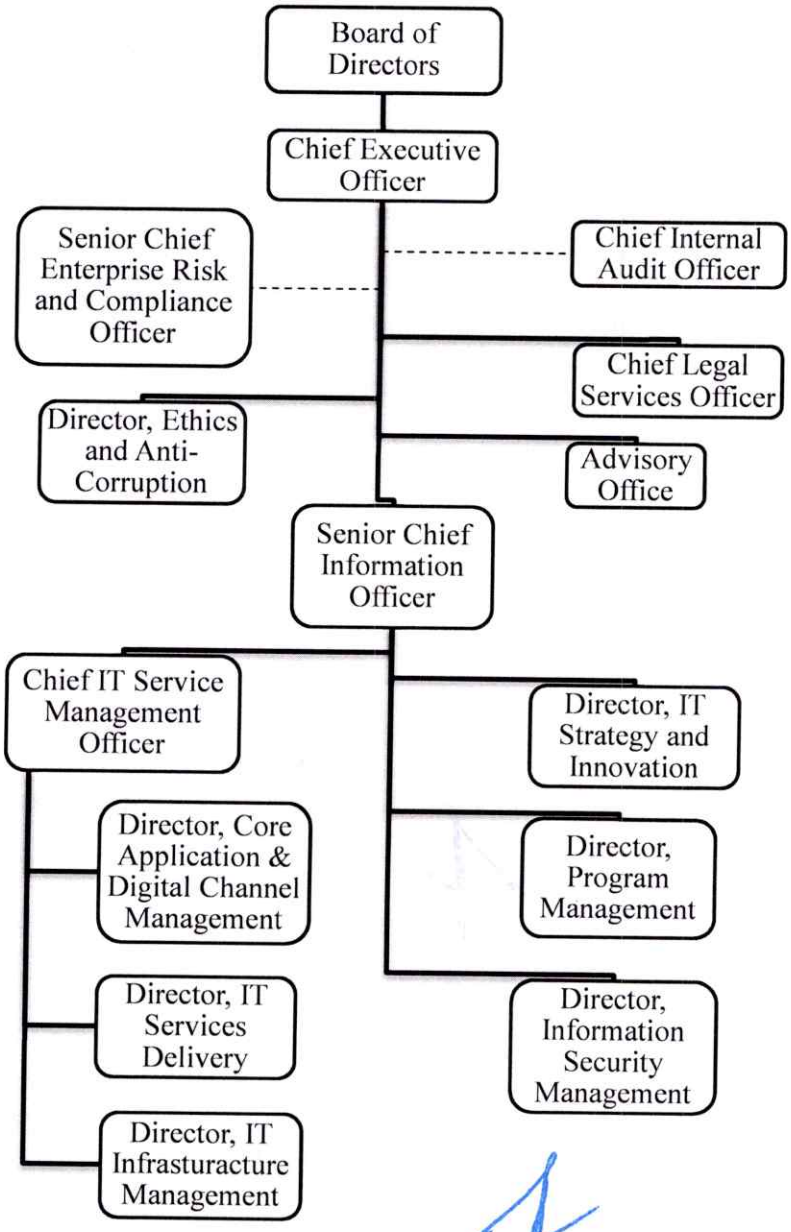
6. Reference and related documents

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 Systems Asset Management 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

7. Organizational Structure, Roles and Responsibilities

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

7.1.Organizational Structure



7.2.Roles and Responsibilities

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

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

7.2.2 **IT Infrastructure Management Directorate** is responsible for maintaining and updating an asset inventory of Awash Bank's assets.

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

7.2.4 **Business Owner / Asset Owner** is responsible for classification of information in accordance with the rules prescribed in this policy document.

7.2.5 **Asset Custodian** is responsible for:

a. Implementing appropriate controls to protect the confidentiality, integrity, availability and authenticity of sensitive information.
b. for applying security measures in protecting removable storage media.

7.2.6 **Asset Custodian with approval of Asset Owner** is responsible for managing and updating sensitive information of the bank.

7.2.7 **Asset Custodian, with concerned Stakeholders if applicable** is responsible for disposing unused information in a secure way.

7.2.8 **All users** are 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 Classification

8.1.Policy Statement

"Accurate, timely, relevant, and proper classification of information is a critical input for the Bank's effective operations and clients' robust service provisioning. To this end, Awash Bank is highly committed in ensuring a proper and secure classification of information at all times.

Awash Bank recognizes that failure to implement adequate security controls over sensitive information could potentially lead to: irretrievable loss of important information; loss of data integrity or reliability; serious financial consequences; damage to the reputation and/or regulatory and legal penalties. So, it is imperative to define and enforce a secure information classification, hence this policy."

8.2.Policy Details

8.2.1. Classification Criteria

8.2.1.1.The level of confidentiality shall be determined based on the following criteria:

a. The Value of Information - shall be based on impacts assessed during risk assessment.
b. The Sensitivity and Criticality of Information - shall be based on the highest risk calculated for each information item during risk assessment.
c. Legal and Contractual Obligations - shall be based on the list of legal, regulatory and other obligations.

8.2.2. Confidentiality Levels

8.2.2.1.All information shall be classified into the following confidentiality levels:

Confidentiality Level	Labeling	Classification Criteria	Access Restriction
Public	PUBLIC	Making the information public cannot harm the bank in any way.	Information is available to the public
Internal Use	INTERNAL USE	Unauthorized access to information may cause minor damage and/or inconvenience (i.e. limited disruption of the bank's operation, minor damage to reputation and trust) to the bank.	Information is available to all employees and selected third parties
Restricted	RESTRICTED	Unauthorized access to information may considerably damage (i.e. multiple branch offices or multiple business units affected by the incident, moderate damage to reputation and trust) the business and/or the bank's reputation.	Information is available only to a specific group of employees and authorized third parties

Confidential	CONFIDENTIAL	Unauthorized access to information may cause catastrophic damage (i.e. significant damage to reputation and trust, exposition to lawsuits, payment to damage to affected parties, high public relation and communication costs) to business and/or to the organization's reputation.	Information is available only to individuals in the bank.

8.2.2.2. The basic rule shall be to use the lowest confidentiality level ensuring an appropriate level of protection, in order to avoid unnecessary protection costs.

8.2.2.3. Any unlabeled information shall be classified by default as "confidential" until properly classified and labeled.

8.2.3. List of Authorized Persons:

8.2.3.1. Information classified as "Restricted" and "Confidential" shall be accompanied by a list of authorized persons in which the information owner specifies the names or job functions of persons who will have the right to access that information.

8.2.3.2. The same rule shall applies to the confidentiality level "Internal Use" if people outside the bank will have access to such document.

8.2.4. Handling Classified Information

8.2.4.1. All persons accessing classified information shall follow the rules listed in the following table. **HR Operations Directorate** shall initiate disciplinary action each time the rules are breached or if the information is communicated to unauthorized persons.

Asset categories	Internal Use	Restricted	Confidential
Paper Documents	1. If sent outside the bank, the document shall be sent as registered mail 2. Documents shall only be kept in rooms without public access. 3. Documents shall be frequently removed from printers or fax machines	1. The document shall be stored in a locked cabinet 2. Documents shall be transferred within and outside the Bank only in a closed envelope 3. If sent outside the Bank, the document shall be mailed with a return receipt service 4. Documents shall immediately be removed from printer or fax machines 5. Only the document owner shall copy the document 6. Only the document owner shall destroy the document	1. The document shall be stored in a safe 2. The document shall be transferred within and outside the bank only by a trustworthy person in a closed and sealed envelope 3. Faxing the document shall not be allowed 4. The document shall be printed out only if the authorized person is standing next to the printer 5. Only the document owner shall copy the document

			6. Only the document owner shall destroy the document
Electronic Documents	1. Access to the information system where the document is stored shall be protected by a strong password 2. The screen on which the document is displayed shall be automatically locked after 5 minutes of inactivity	1. Access to the information system where the document is stored shall be protected by a two factor authentication 2. When files are exchanged via services such as FTP, instant messaging, etc., they shall be password protected 3. Only the document owner shall erase the document	1. The document shall be stored in encrypted form 2. Access to the information systems where the document is stored shall be protected by two factor authentication using smart cards, tokens, or biometric readers 3. The document shall be stored only on servers which are controlled by the Bank 4. When files are exchanged via services such as FTP, instant messaging, etc., they shall be encrypted 5. Only the document owner shall erase the document
Information Systems	1. Access to the information system shall be protected by a strong password 2. The screen shall be automatically locked after 5 minutes of inactivity. 3. The information system shall only be located in rooms with controlled physical access	1. Access to the information system shall be controlled through a two-factor authentication 2. Users shall log out of the information system if they have temporarily or permanently left the workplace 3. Data shall be erased only with an algorithm which ensures secure deletion 4. The information system shall only be located in rooms with controlled physical access	1. Access to the information system shall be controlled through a two factor authentication using smart cards, tokens, or biometric readers 2. The information system shall only be installed on servers controlled by the Bank 3. The information system shall only be located in rooms with controlled physical access and identify control of people accessing the room
Electronic Mail	1. The sender shall carefully check the recipient 2. All applicable rules stated under "information systems" apply	1. E-mail shall be encrypted if sent outside the bank 2. The sender shall carefully check the recipient 3. All applicable rules stated under "Information Systems" apply	1. All E-mails shall be encrypted 2. The sender shall carefully check the recipient 3. All applicable rules stated under "Information Systems" apply
Electronic Storage Media	1. Media or files shall be password protected 2. If sent outside the Bank, the medium	1. Files on the Media shall be encrypted 2. Media shall be stored in a locked cabinet	1. Files on the Media shall be encrypted 2. Media shall be stored in a safe

	shall be sent as registered mail 3. The medium shall only be kept in rooms with controlled physical access	3. If sent outside the Bank, the medium shall be mailed with a return receipt service 4. Only the medium owner shall erase or destroy the medium	3. Media shall be transferred within and outside the Bank only by a trustworthy person in a closed and sealed envelope 4. Only the medium owner shall erase or destroy the medium
Information transmitted orally	1. Unauthorized persons shall not be present in the room when the information is communicated	1. The room shall be soundproof 2. The conversation shall not be recorded	1. The room shall be soundproof 2. Conversation conducted through a communication channel (e.g.,. online call) shall be encrypted 3. The conversation shall not be recorded 4. No transcript of the conversation shall be kept

8.2.5. Data Masking

8.2.5.1. If the asset owner decides that data exposure is a concern (e.g., personally identifiable information, trade secrets, etc.), the information classification shall be at least "RESTRICTED", and the following additional rules shall be applied to prevent the data from being displayed:

a. Information on paper media: data not needed by the user shall be masked by means of data deletion or data concealment (e.g.,. by covering the text with a black stripe).
b. Information systems or digital documents: data not needed by the user shall be masked by means of data concealment or data substitution (replacing the sensitive data with non-sensitive data).

8.2.6. Information Labeling

8.2.6.1. Confidentiality level shall be labeled in the following way:

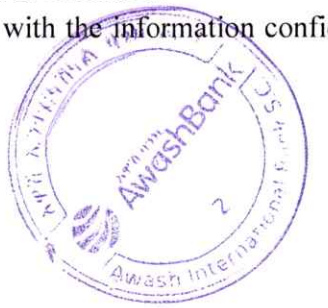
a. **Paper documents** – the confidentiality level shall be indicated in the top right corner of each document page; it shall be also indicated on the front of the cover or envelope carrying such a document as well as on the filing folder in which the document is stored.
b. **Electronic Documents** – the confidentiality level is indicated in the top right corner of each document page.
c. **Information Systems** – the confidentiality level in applications and databases shall be configured and indicated when accessing and using the systems.
d. **Electronic Mail** – the confidentiality level shall be indicated in the e-mail body.

e. **Electronic Storage Media** (disks, memory cards, etc.) – the confidentiality level shall be indicated on the top surface of such a medium.
f. **Information transmitted orally** – the confidentiality level of confidential information to be transmitted in face-to-face communication, by telephone or some other means of communication, shall be communicated prior to the information itself.

8.2.7. Reclassification

8.2.7.1. Asset owners shall review the confidentiality level of their information assets every two years and assess whether the confidentiality level can be changed. If possible, the confidentiality level shall be lowered or escalated.

8.2.7.2. All bank's employees shall comply with the information confidentiality classification level defined above.



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 Auhtorized Persons with access to documents	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
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
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 Classification Policy shall be in force effective from _____ 2023.

End of Document