አዋሽ ባንክ
AwashBank

Circular No. 37/2023

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:- Access Control Policy

Please find enclosed herewith the Access Control Policy for your perusal and implementation.

Softcopy of the Access Control 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:- Access Control 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 2: Access Control Policy

April 2023

Information

Title	Code	Classification	Version	Status
Access Control 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.
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.
Need to Know	A user is only granted access to the information he needs to perform his Need to Know tasks (different tasks/roles mean different need-to-know and hence different access profiles).
Need to Use	A user is only granted access to IT facilities (e.g., equipment, applications, procedures and rooms) he needs to perform hi task/job/role.
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.
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.
Provisioning	A process of assigning or revoking access rights for users to information, systems and services.
Privileged Accounts	Are systems or application accounts that have advanced permissions on such systems or applications.
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

The basic access control principle is that access to all systems, networks, services, and information is forbidden, unless expressly permitted to individual users or group of users.

Access controls are necessary to ensure only authorized users can obtain access to an organization's information and systems.

Access controls manage the admittance of users to system and network resources by granting users access only to the specific resources they require to complete their job related duties.

Access control procedures should cover all stages in the life-cycle of managing user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention is required, where appropriate, to the need of controlling the allocation of privileged access rights, which may allow users to override system controls.

3. Purpose

The main purpose of this policy document is to limit access to information and information processing facilities, ensure authorized user access and to prevent unauthorized access to systems and services, make users accountable for safeguarding their authentication information, and prevent unauthorized access to systems and applications.

4. Scope of Applicability

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

5. Users

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

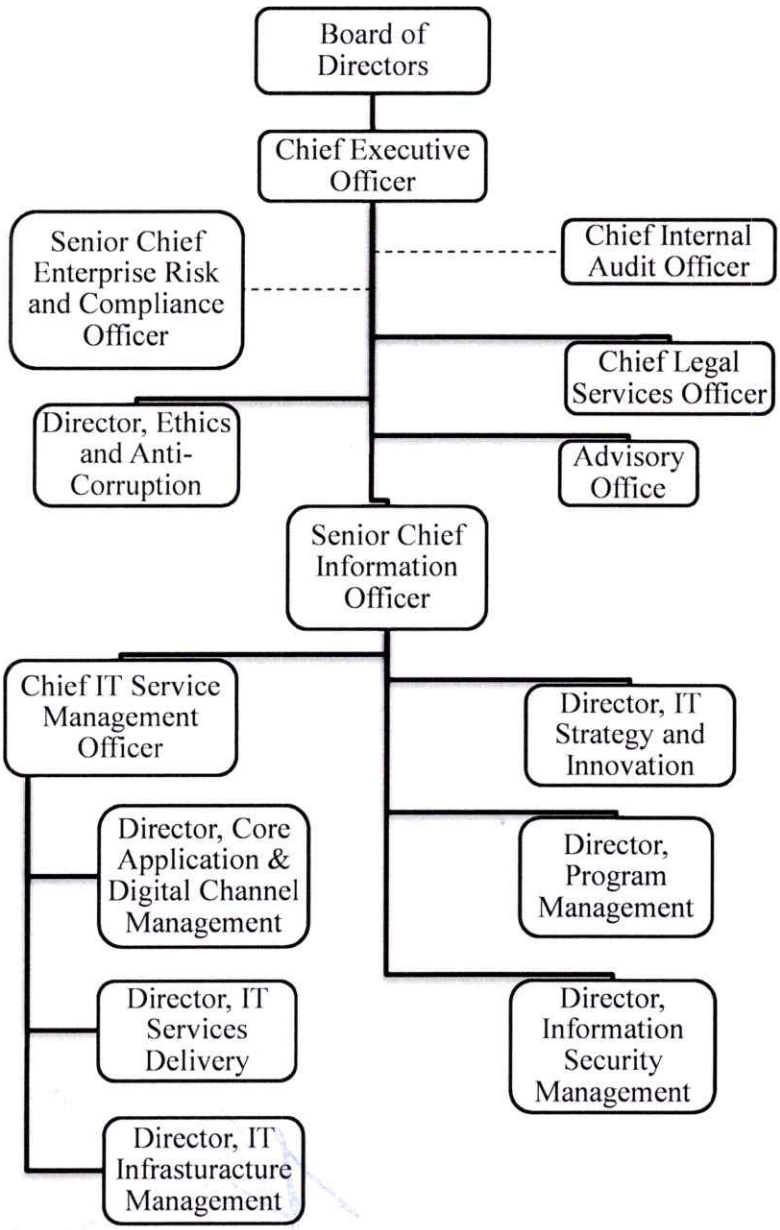
6. Reference and related documents

a. ISO/IEC 27001 Standard
b. Awash Bank Information Security Policy
c. Awash Bank Information Systems Asset Management Policy
d. Awash Bank Human Resource Security Policy
e. Awash Bank Information Security Risk Management Policy
f. Awash Bank Change Management Procedure/Process

7. Organizational Structure, Roles and Responsibilities

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

7.1.Organizational Structure



7.2.Roles and Responsibilities

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

a. Ensuring the protection of information/ infrastructure systems, according to the technological mechanisms defined by the system/ application design team.

b. Investigating breaches of security controls, and implementing additional compensating controls when necessary.

7.2.2 **HR Operations Directorate** is responsible for ensuring resigned or terminated employee return all Awash bank's assets interested before they complete termination process.

7.2.3 **Asset Owner** is responsible for:

a. Determining the required access rights of users to assets.

b. Approving user access registration form.

7.2.4 **Asset Owner or Asset Custodian** is responsible for revoking access rights (logical and physical) to assets upon employee termination or change.

7.2.5 **Asset Custodian** is responsible for:

a. Implementing proper controls to protect assets.

b. Reviewing user access rights and privileges in a regular basis.

7.2.6 **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 security incidents to **Information Security Management Directorate**.

8. Access Control

8.1.Policy Statement

"Access to Awash Bank's Information and Information system shall be controlled on the basis of business and security requirements. Access to information assets and rules governing such access shall be defined and documented. This policy specifies rules for access to the bank's systems, services and facilities, while the Information Systems Asset Management policy defines rules for access to individual documents and records of the bank."

8.2.Policy Details

8.2.1. Access Control

8.2.1.1. Access to information shall be controlled based on business and security requirements and the access control rules defined for each bank's system. These rules shall include the followings:

a. Both logical and physical access controls.
b. Security requirements of bank's business applications.
c. An identified business requirement for the user to have access to the information or business process (both 'need-to-know' and 'need-to-use' principles).
d. All access is denied unless specifically approved under the provisions of this policy.
e. Changes in user permission whether performed automatically or by an administrator.
f. Legal and/or contractual obligation to restrict and protect access to bank's systems.

8.2.1.2. Access for contractors or third parties personnel to bank's business information assets shall be provided only based on a contractual agreement. This agreement shall include, but not be limited to:

a. The terms and conditions for access provided.
b. The security responsibilities of the contractors or third parties personnel.
c. Agreement by the contractors or third parties personnel to abide to bank's information security policies.

8.2.1.3. Access to networks and network services shall be authorized and controlled based on business, security requirements and access control rules defined for each network. These rules shall take include the followings:

a. Security requirements of the network or network services.
b. An identified business requirement for the user to have access to the network (e.g., use of VPN or wireless network) or network services ('need-to-have' principle).
c. The user's security classification and the security classification of the network.
d. The user's authentication requirements for accessing various network services.
e. Monitoring and managing of the use of network services.
f. The authorization mechanisms for determining who is allowed to access which networks and network services.

8.2.1.4. All computers shall be not connected to bank network and be allowed full access to all network resources and the Internet unless they fulfil with the network access control requirements as follows:

a. Security policies of operating system.
b. Updated antivirus definitions.
c. Firewall security rules.

8.2.1.5. Access to shared folders shall consider the followings:

a. Only authorized for specific users.
b. Only used for bank's business purpose.
c. Sharing any non-related business materials (e.g., photos, videos, audio files, etc.) shall not be permitted.

8.2.2. Identity Management

8.2.2.1. Access to Information, systems, computing assets and facilities shall be controlled through a formal user registration process beginning with official request from Director, Manager.

8.2.2.2. The official request for user account creation shall be made in writing (email or hard copy) by the user's departmental directorate/ manager.

8.2.2.3. Each user shall be granted and identified by a unique user ID/User name.

8.2.2.4. All users shall have a unique User ID based on a standard naming convention, for accessing Awash Bank information systems.

8.2.2.5. All users shall be assigned a unique official email ID for business use.

8.2.2.6. While creating User IDs, details like Full name, job position, date of creation, approver, purpose of access, privilege level required, expiry date (If applicable) etc. shall be recorded.

8.2.2.7. Procedures shall be established to link all access to system components to individual user.

8.2.2.8. Appropriate authorization from the **IT Service Delivery Directorate** shall be obtained prior to creating the User IDs on the information systems of the Bank.

8.2.2.9. Access privileges to the users shall be granted only in accordance with the user's role and post appropriate approval.

8.2.2.10. An audit trail shall be kept of all requests to add, modify or delete user accounts/IDs and access rights.

8.2.2.11. Redundant user accounts shall be removed or disabled.

8.2.2.12. Redundant, shared or group user IDs shall not be allowed.

8.2.2.13. The user accounts of terminated employees shall be removed or disabled immediately.

8.2.3. Access Rights

8.2.3.1. All authorized user accessing bank's assets shall be defined and documented.

8.2.3.2. Authorizations process shall be tracked and logged as follows:

a. Date of authorization.
b. Identification of individual approving access.
c. Description of access privileges granted.
d. Description of why access privileges granted.

8.2.3.3. The provisioning process for assigning or revoking access rights for users shall consider the followings:

a. Obtaining a proper authorization from the system or service's owner.
b. Segregation of duties to ensure a proper access level is given.
c. Access rights are not activated until an authorization process is completed.
d. Records reflecting all user access rights are centrally kept up-to-date.
e. Updating users access rights based on bank's employees roles and responsibilities.
f. Reviewing users access rights in a regular basis.

8.2.3.4. **Asset Custodian** shall grant users access to bank's systems and services in accordance with their business role and job description (i.e., access right profiles).

8.2.3.5. Upon detection of any misconduct of privileged access rights, **Asset Custodian** shall restrict such privileges.

8.2.3.6. All bank's users' access rights shall be reviewed in accordance with the formally approved User Physical and Logical Access Control Procedure.

8.2.3.7. Asset Custodian shall establish a user access rights review plan that includes:

a. Awash Bank's systems to be reviewed.
b. The review frequency.

8.2.3.8. **Asset Custodian** shall review the following access privileges:

a. Access profiles for high risk systems (mission critical systems) every three months.
b. Access profiles for medium risk systems every six months.
c. Access profiles for normal risk systems on an annual basis.

8.2.3.9. Department Manager shall promptly report all significant changes in employees' duties and/or employment status to Human Resources Department / Administration Unit/.

8.2.3.10. When an employee permanently leaves the bank:

a. System administrators shall be notified.
b. All bank's access privileges shall be promptly terminated.
c. **Asset Custodian**, unless notified to the contrary, shall purge all files held in the employee's directory one month after employment termination.

8.2.4. Management of Privileged Access Rights

8.2.4.1. Creation and allocation of privileged user accounts/IDs on Awash Bank's information systems shall be controlled through a formal authorization process.

8.2.4.2. Creation and allocation of privileged user accounts authorization process shall cater the following:

a. The privileges associated with each system (e.g. operating systems, databases, applications etc.) and their corresponding users shall be identified and recorded.
b. Privileges shall be allocated to individuals on a 'need-to-use' basis in strict adherence to the authorization process for granting privileged access.
c. A record of all privileged accounts used on Awash Bank information systems shall be appropriately maintained on hardcopy or softcopy.
d. Defining expiry requirements for all access rights shall be mandatory.
e. Changes made to privileged accounts shall be logged.

8.2.4.3. Users shall not have access to administration account or privileges on their local machines.

8.2.5. Authentication of Information

8.2.5.1. All Awash Bank's systems shall require identification and authentication through a proper secret authentication information method (e.g., passwords, token IDs, smart cards or biometrics).

8.2.5.2. Prior to allowing user access to any Awash Bank's system or application, a password authentication method shall be implemented as follows:

a. Password shall be a minimum of 8 characters' length for normal users and 12 characters for IT administrators (e.g., system admin, application admin, DB admin and network admin).
b. Password shall be combination of at least three of the four followings:
   - At least one lower case alphabetic character (a-z);
   - At least one upper case alphabetic character (A-Z);
   - At least one number (0-9);
   - At least one special character (e.g., @#$%^&*()_+|~-=\`{}[]:";'<>/).
c. Passwords shall not contain user ID.
d. Blank password shall not be allowed.
e. Users shall be required to change their password immediately after their first login to any system (i.e., It shall be configured to prompt a user to choose another password before continuing with his session).
f. The system shall lock User account shall be locked fort 3 minutes after 3 unsuccessful attempts by the system.
g. Password change shall be enforced (by the operating system or the application) at least every 30 days. Re-use of the same password shall not be allowed.
h. Initial password shall be only used one time (i.e., it shall be valid only for the involved user's first login) and shall be expired at 23:59:59 of the date issued.
i. Password shall be stored and transmitted in protected (e.g., encrypted or hashed) form, if possible.

8.2.5.3. Passwords shall be immediately changed if there is any suspicion of password compromise; and this shall be reported immediately **to IT Service Delivery Directorate** and **Information Security Management Directorate**.

8.2.5.4. Users shall be accountable for any activity associated with their access rights.

8.2.5.5. Users shall not capture or otherwise obtain passwords, decryption keys or any other secret authentication method that could permit unauthorized access.

8.2.5.6. Users shall not do the following:

a. Reveal a password over the phone to anyone.
b. Reveal a password in an email message.
c. Reveal or distribute a password to others even to IT Administrators or his boss.
d. Talk about a password in front of other.
e. Hint at the format of a password:
   - Name of family, friends and co-workers.
   - Birthday, address and phone number.
   - Patterns: "aaabbb" and "1112222".
f. Reveal a password on questionnaires or security forms.

g. Share a password with family members.
h. Reveal a password to co-workers while on vacation.
i. Write a password on a piece of paper and left in a place where unauthorized users are able to discover them.

8.2.5.7. **Asset Custodian** shall ensure that:

a. Passwords are always encrypted when held in storage or in system logs on any Awash Banks system.
b. Passwords are not to be stored in internet browsers (i.e., cookie on user's workstations are not set for automatic password completion and login).
c. Systems are designed, tested and controlled to prevent the retrieval of and the unauthorized use of stored passwords.

8.2.5.8. The bank shall adopt an interactive system for managing passwords in order to:

a. Enforce a quality of passwords.
b. Enforce regular password changes as needed.
c. Maintain a record of previously used passwords.
d. Hide passwords on the screen when being entered.
e. Isolate password files from application system data.
f. Encrypt password when being stored and transmitted.

8.2.6. Information Access Restriction

8.2.6.1. Appropriate controls shall be defined to control application systems functions as follows:

a. Limiting outputs information.
b. Restricting access to information based on a user access profile.
c. Defining proper access privileges required (e.g., read, write, delete and execute).
d. Implementing logical and physical access isolation between different critical bank's systems.

8.2.7. Secure Authentication

8.2.7.1. Login into bank's critical system, databases, communication devices and operating systems shall be based on a formal secure logon procedure.

8.2.7.2. All systems shall display a general notice warning message that access to bank's systems is granted to authorized users only.

8.2.7.3. The logon process on any system shall display only the limited information about the system and its purposed use.

8.2.7.4. When strong authentication and identification is required, authentication methods other than passwords (e.g., token IDs, smart cards or biometrics) shall be implemented.

8.2.7.5. All systems shall limit the number of unsuccessful logon attempts allowed; the following shall be considered:

a. Recording both successful and unsuccessful attempts.
b. Forcing a time delay before further logon attempts are allowed or rejecting any further attempts without specific authorization.

c. Sending an alarm message to the system Administrator or security solutions such as SIEM (Security Incident and Event Management) if the maximum number of logon attempts is reached.

8.2.7.6. **Asset Custodian/System Administrators** (e.g., system admin, application admin, DB admin and network admin) shall review all unsuccessful log attempts in a periodically basis.

8.2.8. Use of Privileged Utility Programs

8.2.8.1. System utilities shall be restricted from all users unless the user has received a written authorization from **Asset Owner**.

8.2.8.2. All access to system utilities shall be logged and reviewed by designated authority.

8.2.8.3. Access to and use of system programs shall be restricted and controlled.

8.2.8.4. All unnecessary system utilities and software shall be removed.

8.2.9. Access to Source Code

8.2.9.1. Access to source codes, configurations and relevant items (e.g., designs, specifications, verification plans and validation plans) shall be documented and restricted to an authorized personnel.

8.2.9.2. The designated personnel shall ensure that all source codes are compiled, controlled and maintained centrally.

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
Records of regular review of access rights (of different assets)	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	Minimum 2 years
Records of Roles and Privileges on the Core-Banking Service	IT Service Delivery Directorate, Core Application and Digital Channel Management Directorate, IT Infrastructure Management Directorate, Information Security Management Directorate	IT Service Delivery Directorate, Core Application and Digital Channel Management Directorate, IT Infrastructure Management Directorate, Information Security Management Directorate	Only IT Service Delivery Directorate, Core Application and Digital Channel Management Directorate, IT Infrastructure Management Directorate, Information Security Management Directorate can publish and edit Read access to other is in need-to-know basis only Malware protection	Minimum of 1 year
User Access Right Record	Asset Custodian's 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	5 Years
Privileged Access Right Record	Asset Custodian's computer / cabinet	IT Infrastructure Management Directorate	Only IT Infrastructure Management Directorate can publish and edit	5 Years

			Read access to other is in need-to-know basis only Malware protection	
Access Request Record	Asset Custodian's 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
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 Years
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 Years

Only **Asset Owner/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 Access Control Policy shall be in force effective from _____ 2023.

End of Document