This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the outlined image.

Identity and Access Management Policy Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press "Ctrl" + "H" keys simultaneously.
- Enter "<organization name>" in the Find text box.
- Enter your organization's full name in the "Replace" text box.
- Click "More", and make sure "Match case" is ticked.
- Click "Replace All".
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>’s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This policy aims to define the cybersecurity requirements related to identity and access management for <organization name>’s information and technology assets, in order to minimize the cybersecurity risks resulting from internal and external threats in <organization name> and ultimately preserving confidentiality, integrity and availability.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy covers all information and technology assets in the <organization name> and applies to all personnel (employees and contractors) in the <organization name>.

Policy Statements

1 General Requirements

1-1 An access management procedure must be documented and approved to illustrate, monitor, and implement the creation, modification, and revocation of access privileges to <organization name>'s information and technology assets.

1-2 Users’ identities must be created according to <organization name>’s legal and regulatory requirements.

1-3 User authentication and validation must be performed using a username and password before granting users access to <organization name>’s information and technology assets.

1-4 Users' identities, accounts, and privileges must be kept confidential, and users (personnel, third parties, and other users) must be required to maintain the privacy of such information.

1-5 An authorization matrix must be documented, approved, and reviewed based on the following identity and access management principles:

- Need to know and need to use.
- Segregation of duties.
- Least privilege.

1-6 Authentication controls for all information and technology assets in <organization name> must be implemented via an automated and centralized access control system, such as Domain services -Active Directory.

1-7 Generic user accounts must not be allowed to access <organization name>'s information and technology assets.

1-8 Secure session management must be ensured, including session authenticity, lockout, and timeout.

1-9 Systems and sessions must be configured to automatically timeout after a specific period (Session Timeout), as per <organization name>'s approved Identity and Access Management Standard.

1-10 Systems and sessions must be configured to temporarily lockout after a specific number of unsuccessful login attempts, as per <organization name>'s approved Identity and Access Management Standard.

1-11 Users' accounts that have been inactive for a specific period must be disabled, as per <organization name>'s approved Identity and Access Management Standard.

1-12 All identity and access management systems must be configured to forward logs to a central logging and monitoring system as per the Cybersecurity Event Logs and Monitoring Management Policy.

1-13 Direct access to and handling of critical systems' databases must not be granted to users; except Database Administrators which can access the databases only through the applications. Procedures must be in place to prevent Database Administrators from accessing classified and sensitive data, as per <organization name>'s approved Database Security Policy.

1-14 Procedures to manage service accounts must be documented and approved. Service accounts between applications and systems must be periodically reviewed and securely managed, and interactive users' access through Interactive Login must be disabled.

1-15 Users’ privileges for remote work must be managed based on business needs, considering system criticality, privilege levels, and the types of devices used by personnel to work remotely, in line with the relevant legal and regulatory requirements.

1-16 Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and efficient and effective use of identity and access management protection requirements.

2 Granting Access

2-1 User Accounts Access Requirements

2-1-1 Access must be granted based on the user request by an approved form from <cybersecurity function> or by the approved system from the line manager and the system owner. The request must define the system name, request type, access type, privilege, and duration (in case the access privilege is temporary).

2-1-2 Access to any of <organization name>'s information and technology assets must be granted in line with the roles and responsibilities of the user, after obtaining the required approvals.

2-1-3 User IDs must be created following a standardized naming convention format that enables tracking the activities conducted by the user ID and linking them with the user (e.g., <first name initial> dot <last name>, or a pre-defined employee number with the <human resources function>).

2-1-4 Concurrent logins from multiple workstations must be disabled.

2-1-5 The number of allowed unsuccessful login attempts to the system must be defined to prevent password guessing attacks as per <organization name>'s approved Identity and Access Management Standard.

2-2 Privileged Access Requirements

In addition to the controls stipulated in the “User Accounts Access Requirements” section, the below controls must be applied to privileged accounts:

2-2-1 Administrator privileges must be assigned based on job duties, while taking into account the segregation of duties principle.

2-2-2 Password history must be enabled to track the number of passwords that have been changed.

2-2-3 Default accounts, specifically privileged ones such as “Root”, “Admin”, and “Sys id”, must be renamed.

2-2-4 Privileged accounts must be prevented to be used for day-to-day operations and connected to the Internet.

2-2-5 Privileged users' accounts on information and technology assets must be authenticated through a Multi-Factor Authentication (MFA) mechanism, using at least two factors, as per <organization name>'s approved Identity and Access Management Standard.

2-2-6 A Privileged Access Management (PAM) solution must be used to maintain and manage privileged accounts.

2-2-7 Access to critical systems and the systems that are used to manage and monitor critical systems must require an MFA mechanism for all personnel.

2-3 Remote Access to <organization name>'s Networks

2-3-1 Remote access to information and technology assets must be granted after obtaining permission from the <cybersecurity function>, and it must be restricted using an MFA mechanism through secure channels that are approved in <organization name>.

2-3-2 Event logs of remote access sessions must be maintained, and related activities must be monitored continually based on the criticality of information and technology assets.

2-4 Revoking and Changing Access

2-4-1 The <human resources function> must notify the <information technology organization> to take necessary actions when a user is transferred, assigned new duties, or when the user's contract with <organization name> ends or is terminated. The <information technology organization> must revoke or update the user's account and access based on the newly assigned role. These measures must be automated as much as possible.

2-4-2 The event logs of user whose access is revoked must be prohibited of deletion, and they must be maintained as per <organization name>'s approved Cybersecurity Event Logs and Monitoring Management Policy.

2-5 Identity and Access Management Review

2-5-1 User IDs and their use for information and technology assets must be reviewed <annually>. User IDs and their use for critical systems must be reviewed at least every three months.

2-5-2 User profiles and their use for information and technology assets must be reviewed <annually>. User profiles and their use for critical systems must be reviewed at least every three months.

2-6 Password Management

2-6-1 A secure password policy with high standards must be applied for all accounts in <organization name>, as per its approved Identity and Access Management Standard in <organization name> and other relevant legal and regulatory policies and requirements.

2-6-2 Users must be notified before the expiration of their passwords to remind them to change their passwords before the expiration.

2-6-3 Previously used passwords must not be used.

2-6-4 All information and technology assets must be configured to force users to change their temporary passwords upon their first login.

2-6-5 Default passwords for all information and technology assets must be changed before their deployment to the production environment.

2-6-6 Simple Network Management Protocol (SNMP) default community strings (such as "public," "private" and "system") must be changed and must be different from the passwords used to log into the respective technology assets.

2-7 Password Protection

2-7-1 All <organization name>'s information and technology asset passwords must be encrypted to be rendered unreadable during entry, transmission, and storage as per <organization name>'s approved Cryptography Policy.

2-7-2 Passwords must be masked on the screen when being entered.

2-7-3 "Remember Password" feature must be disabled on <organization name>'s systems and applications.

2-7-4 Dictionary words must not be allowed to be used as is in the passwords.

2-7-5 Passwords must be delivered to users using a secure and reliable method following defined and approved procedures.

2-7-6 If a user requests a password reset by phone, Internet, or any other method, the user's identity must be authenticated before resetting the password through defined and approved methods, including but not limited to activating and updating security questions.

2-7-7 The passwords of privileged accounts and service accounts must be protected and stored securely in a proper location (in a sealed envelope in a safe box) or using a Privilege Access Management (PAM) solution.

Roles and Responsibilities

1- **Policy Owner:** <head of cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

3- **Policy Implementation and Execution:** <information technology function>, <human resources function>, and <cybersecurity function>

4- **Policy Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- <Head of cybersecurity function> will ensure the compliance of <organization name> with this policy on a regular basis.

2- All personnel of <organization name> must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action according to <organization name>'s procedures.