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

Insert organization logo by clicking on the outlined image.

Identity and Access Management Standard Template

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.

Choose Classification

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

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 standard aims to define the detailed cybersecurity requirements related to the identity and access management of <organization name>'s systems, data and information to minimize cybersecurity risks resulting from internal and external threats at <organization's name> in order to preserve confidentiality, integrity and availability.

The requirements in this standard 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 standard covers all <organization name>'s information and technology assets (e.g., workstations, mobile devices, and servers) and applies to all personnel (personnel and contractors) in the <organization name>.

Standards

1	User identity
Objective	To manage a unique identifier (UserID) for individuals using <organization name> IT systems.
Risk implication	Lack of unique UserID may result in a loss of user accountability, inability to track user activities and poor control over access rights and access privileges.
Requirements	
1-1	<organization name> must appoint a process owner to define the process for issuing all personnel of <organization name> with a unique UserID, maintain it and change the process as directed by business and/or statutory requirements.
1-2	A process must be defined for issuing all personnel with a unique identifier (UserID) for use with <organization name> IT systems.

1-3	Minimum requirements for UserID must be defined to consistently provide UserIDs with appropriate and consistent attributes.
1-4	A secure password standard, with minimum requirements, must be defined (see section 3-5).
1-5	The process for issuing all personnel of <organization name> with a unique UserID must include the following minimum requirements: a) a RACI chart defining who can make and authorize requests for issuing UserID b) how a request for a new UserID is to be submitted c) who can request a new UserID (e.g. HR) d) who can create a UserID and grant access rights e) who can authorize requests (e.g. line manager) f) how access rights are to be associated with a UserID (e.g. based on role or location) g) require the use of template UserIDs for ID creation h) how the UserID and password are to be issued i) how the UserID can be disabled j) maximum time a request to create or disable a UserID can take k) maximum time within which all access associated with the UserID must be revoked, if required l) maximum time, thereafter, within which UserID must be deleted m) how the issue of a UserID is recorded and protected
1-6	All personnel must be issued with a unique identifier (UserID) for use with <organization name> IT systems. These identifiers must not be generic or shared.
1-7	A process must be implemented that ensures all changes are auditable and logged; the logs must be retained for at least 12 months.

2	User authorization
Objective	To enforce authorization of users to use <organization name> IT systems (including the cloud).
Risk implication	A lack of authorization may result in users gaining access to systems or data and information inappropriate to the user's job, role, seniority or security clearance.
Requirements	
2-1	A process owner must be appointed to define the process for authorizing users before they are granted access privileges to <organization name> IT systems.
2-2	A process for authorizing users must be defined and documented. The process must include, at a minimum: a) the request mechanism for authorizing a user and agreed approvers (roles) b) associating access privileges with defined users (e.g., using unique identifiers such as User IDs) to provide individual accountability c) defining and assigning users with default access d) relevant owners pre-approving standard accesses for basic roles (role-based access control RBAC) e) assigning access based on the principle of Need-to-Know and Need-to-Use, Least Privilege (i.e., 'none' if access is not required and authorized) and Segregation of Duties (see section 4) to the different systems including but not limited to servers, databases, external web applications, and logging systems f) ensuring redundant identifiers (e.g., User IDs) are not reissued for use g) authorization of user access in exceptional circumstances (e.g., where access control mechanisms are not available, practical or safe or where technical functionality is not available)

2-3	Approval for authorization must be obtained from the relevant owners and applied to all users.
2-4	A file or database containing details of all authorized users must be maintained by authorized individuals.
2-5	The file or database containing details of all authorized users must be protected against unauthorized access, unauthorized change and unauthorized disclosure by logical and physical controls.
2-6	Define the process to review access privileges of authorized users: a) to ensure that access privileges remain appropriate b) to check that redundant authorizations and associated accesses have been deleted (e.g., for individuals who have changed roles or left the organization) c) on a regular basis (i.e., at least once every year) d) more frequently for users with special/elevated access privileges, or when involving data classified as secret & above (i.e., every six months) e) more frequently for user access to critical systems (i.e., every three months)
2-7	User session must be terminated automatically after meeting defined conditions, such as session timeout on different systems including but not limited to databases, external web applications, and users' workstations.
2-8	A central register must be established containing details of all authorized users (current and past), which is maintained by authorized individuals.
2-9	The central register must be protected against unauthorized access, unauthorized change and unauthorized disclosure by logical and physical controls.

3	User authentication
Objective	To enforce secure authentication to <organization name> IT systems.
Risk implication	Lack of authentication may result in users being able to masquerade as other users, bypass access rights and access systems or data and information inappropriate to the user's job, role, seniority or security clearance.
Requirements	
3-1	Authentication to <organization name> IT systems (including but not limited to the cloud, databases, network devices, and wireless network devices) must be enforced by requiring the use of a unique identifier and supporting factor(s) (e.g., passwords/phrases, tokens or one-time passwords).
3-2	Authentication mechanisms must be configured so that: a) all login information is required to be entered before validation b) passwords and other login information is masked during input c) the number of unsuccessful login attempts is limited to three incorrect attempts; the user is temporary locked out, forcing a reset of the authentication information (not the UserID) d) all authentication information is stored and processed in a secure manner (e.g. by using encryption) e) all login attempts are recorded and stored in a secure manner
3-3	The secure use of authentication information (UserID, passwords and other authentication factors) must be enforced
3-4	Access logs must be reviewed at least once every six months for multiple login attempts using the same UserID, and for the

	same UserID being used from different terminals (concurrent logins).
3-5	The password standard for the users' workstations must implement the following minimum rules: a) password length must be at least 8 characters b) passwords must include at least one of each: lower-case letters (a-z), capitalized letters (A-Z), numbers (0-9) and special characters (e.g. £$*) c) passwords must be changed on a regular basis – at least every 90 days – where in use (not required if multi-factor authentication is implemented) d) the last 12 passwords used may not be repeated e) autogenerated passwords must not follow a fixed pattern
3-6	All default usernames and passwords for new systems must be changed before being used in the production environment.
3-7	Default/non-interactive/unneeded accounts on different systems including but not limited to servers, databases, external web applications, logging systems, network devices, wireless network devices, and users' workstations must be disabled or renamed.
3-8	Implement <organization name> approved multi-factor authentication for users in the following cases: a) for domain access b) for critical systems, or systems used for managing critical systems c) critical servers d) for privileged users (including privileged cloud users) e) for web applications f) for databases g) for network devices h) for wireless network devices i) for logging systems

4	Segregation of duties
Objective	To enforce segregation of duties and prevent combinations of access rights which grant users, unintentionally, with excessive access rights.
Risk implication	Lack of segregation may allow users to conduct transactions which are fraudulent, in error, or that exceed the user's seniority or authority.
Requirements	
4-1	The types of activities that require segregation of duties and access rights must be defined.
4-2	The list of activities must include (but is not limited to) the following, as users may only have one set of rights from any list: a) duties of running business applications, systems and network b) duties of those responsible for designing, developing and testing business applications, systems and networks c) designing, implementing and assuring controls d) designing, reviewing and operating code and configurations e) access to development, test, user acceptance, and production environments (production data must not be made available in non-production environments) f) initiating (or changing) and approving critical or sensitive functions (e.g., payments, and pricing) g) requesting, approving and provisioning access rights h) initiating, approving and implementing changes to IT systems

4-3	Access control arrangements, standards and procedures must be documented. These arrangements, standards and procedures must take account of: a) the cybersecurity requirements, data classifications, agreements with application owners, requirements set by system owners, and legal, regulatory and contractual obligations b) the need to achieve individual accountability, apply additional controls for users with special access privileges, and provide segregation of duties
4-4	The activities requiring segregation of duties and access control arrangements must be reviewed: a) at least once a year for all users b) at least every three months for privileged users
4-5	Access rights found to be in breach of segregation of duties or access control standards must be revoked immediately.
4-6	A review to determine how the breach of segregation of duties occurred must be held.
4-7	Where required, the segregation of duties and their enforcement must be updated to reflect changes identified in the review.
5	Access management
Objective	To manage the access privileges for standard users of <organization name> systems.
Risk implications	Poorly defined access privileges may allow users to conduct transactions, enter or alter data and information, or alter the operating of the system inappropriate to the user's job, role, seniority or security clearance.
Requirements	
5-1	A process owner must be appointed to own and define the process for standard user access provisioning.

5-2	The process for system access provisioning must be defined and documented to set out how application access privileges are requested, approved, provisioned and maintained.
5-3	The process must include the following minimum requirements: a) how a request for system access (or a change to such access) is to be submitted b) who can request system access for a user (e.g. user, line manager, etc.) c) who can authorize system access (e.g., the business application owner) d) who can create a system user and grant access rights e) how access rights are associated with a system user (i.e., based on role) f) how the system is to be accessed g) how the system access is issued h) how the system access can be revoked i) maximum time a request to create, change or revoke system access can take j) how the issue of system access is recorded and protected
5-4	System access privileges must be reviewed at least once a year to ensure they are commensurate with user job roles and responsibilities.
5-5	The system owner must conduct a review at least once a year to ensure system access and activity are appropriate and valid, e.g. data extraction from the system. Collected log data may be used in this review.
5-6	User system access privileges must be reviewed to ensure they do not breach any segregation of duty rules that are specified by the business.
5-7	All user system access must be configured in accordance with the principle of least privilege.

5-8	Inactive application user accounts must be disabled after 30 days of continuous inactivity, after getting feedback from HR in regards to reasons of inactivity.
5-9	Access to systems must be restricted to management zone or management VLAN only.
5-10	A joiner, mover, leaver (JML) process must be implemented to manage the identity lifecycle of a user and allow the necessary permissions to systems: a) Access must be granted automatically based on pre-approved access permissions for new personnel based on job roles b) Access must be reviewed and accordingly modified upon personnel transfer c) Access must be disabled to systems upon personnel termination
6	Privileged user access management
Objective	To manage privileged and super user access to <organization name> to IT systems.
Risk implication	Lack of privileged user may allow users to access systems or data and information inappropriate to the user's job, role, seniority or security clearance. It may also allow users to alter, modify or delete data and information, or make changes to applications, operating systems or other software that can interfere or disrupt normal operation.
Requirements	
6-1	A Privilege Access Management (PAM) solution must be implemented to enforce session-based temporary access to different systems including but not limited to servers, databases and logging systems.
6-2	A process owner must be appointed to define the process to issue and provision privileged access accounts.

6-3	The process must include, as a minimum, the following requirements: a) how a request for privileged access to be added, or changes to such access, is to be submitted b) who can request a privileged UserID c) who can authorize the request for a privileged UserID d) who can authorize the granting of privileged access e) who can create a privileged UserID and grant access rights f) how access rights are associated with a privileged user (e.g. based on role) g) how the privileged access is issued h) how the privileged access can be revoked i) maximum time to grant, change or revoke privileged access j) how the issue of privileged access is recorded and protected k) the frequency of privileged access and account recertification
6-4	A separate naming standard and UserIDs for all privileged access users must be documented and implemented.
6-5	A template for privileged UserIDs must be defined to consistently provide privileged UserIDs with appropriate attributes.
6-6	A separate privileged access UserID must be assigned for each identified privileged user such that it is distinct from the regular UserID of the personnel.
6-7	Passwords used by privileged access UserIDs to access different systems including but not limited to servers, databases, external web applications, and logging systems, must implement the following minimum rules: a) password length must be at least 10 characters

	b) passwords must include at least three of: lower-case letters (a-z), capitalized letters (A-Z), numbers (0-9) and special characters (e.g. £$*) c) passwords must be changed on a regular basis – at least every 30 days d) the last 12 passwords used may not be repeated e) passwords based on the privileged user's personal data, such as date of birth, must not be used
6-8	Activities and tasks requiring privileged access must be defined.
6-9	Privileged access activities and tasks must be undertaken using defined privileged UserIDs.
6-10	Privileged access users must use their privileged UserID to undertake privileged tasks.
6-11	Privileged accounts must be recorded in the privileged access management system.
6-12	Privileged user access must be restricted to identified individuals who require it to perform their job role (e.g. database administrators, finance personnel and HR personnel).
6-13	The use of privileged user accounts must be logged. At a minimum, logs must record: a) User credentials used b) time of login c) source IP (where the login was performed) d) activities performed e) time of logout
6-14	The log data for privileged user accounts must be stored in a secure location, with access limited to authorized personnel, using physical and logical access controls.

6-15	The log data for privileged user accounts must be retained according to retention standards/procedures.
6-16	Access logs must be reviewed at least once a month to check that privileged user credentials are being used for privileged tasks.
6-17	Line management must review privileged access at least every six months to ensure privileged user accounts and activity are appropriate and valid, and confirm, change or revoke assigned privileged access. Collected log data may be used in this review.
6-18	Privileged access to databases must be restricted to database administrators and through applications only (where feasible) and based on the principle of Need-to-know and Need-to-use.
7	Technical account access management
Objective	To manage machine, technical or service (all termed "technical") accounts on <organization name> IT systems
Risk implication	Lack of technical account management may result in these accounts being compromised or used in a manner similar to user accounts, reducing their efficiency and subjecting them to increased threats
Requirements	
7-1	A process owner must be appointed to define the process and template to issue and provision technical accounts.
7-2	A template must be created as a basis for technical accounts to ensure they have consistent configuration and attributes.
7-3	A naming convention for technical accounts must be defined. The convention must ensure that technical accounts can be easily differentiated from user and privileged user accounts.

7-4	A template for technical accounts must have the following defaults: a) be non-interactive b) have a non-expiring password c) have no access, i.e., to productivity tools, web browsers, communication or collaboration tools, the Internet, or other services. d) access to be granted to the account must be least privilege/least capability to perform the assigned tasks, explicitly required, assessed and authorized e) identify owning business unit and account owner f) assign unique identifiers to technical accounts, following the naming convention
7-5	A technical account must be assigned to an owner. The owner is responsible for: a) requesting the creation of the identity and account b) registering the account and its password in the privileged access management system c) requesting access rights for the account d) reviewing the account usage and recertification of access at least once a year e) requesting the revocation of the account when the computing asset is removed from the network
7-6	Assigned access privileges for technical accounts must be documented.
7-7	Assigned access privileges must be approved by an appropriate manager and may subject to additional controls.
7-8	The use of technical accounts must be logged.
7-9	The log data for technical accounts must be stored in a secure location, with access limited to authorized personnel, using physical and logical access controls.

7-10	The log data for technical accounts must be retained according to retention standards/procedures.
7-11	The business unit and account owner must review technical accounts at least once a year to ensure technical account activity and access (recertification) are appropriate and valid. Collected log data may be used in this review.
7-12	The business unit and account owner must confirm, change or revoke technical accounts at least once a year. Collected log data may be used in this review.
7-13	The use of hard-coded passwords must be limited to relevant administrators only as necessary for non-interactive purposes, as well as to recover different systems including but not limited to network devices and wireless network devices that have become disconnected from the network.
8	Remote access management
Objective	To provide secure remote access to <organization name> networks
Risk implication	Insecure remote access can expose <organization name> systems, data and information to the Internet and to unauthorized and unauthenticated users
Requirements	
8-1	A process owner must be appointed to define the process for remote access to <organization name>'s network for personnel and authorized third parties.
8-2	The process for remote access to <organization name> network must be defined and documented.
8-3	The remote access process must include the following minimum requirements: a) the types of devices are permitted to be used for remote access

	b) how a request for remote access (or a change to such access) is to be submitted c) risk assessment of the requested remote access d) who can request remote access (e.g. personnel, line manager) e) who can authorize the issue of remote access (e.g. line manager) f) how access rights are associated with a remote access user g) how the remote access account and associated software are issued h) how the remote access can be revoked i) maximum time a request to create, change or revoke remote access can take j) how the issue of remote access and related software to authorized users is recorded and protected
8-4	Remote access privileges must be reviewed at least once a year to ensure they are aligned with the user job roles and responsibilities.
8-5	All remote access must be configured in accordance with the principle of least privilege.
8-6	All remote login access to <organization name>'s network must be required to encrypt data in transit and use multi-factor authentication.
8-7	The use of remote access by all users must be logged, and this log data must be retained according to the <organization name>'s Cybersecurity Event Logs and Monitoring Management Policy and standard.
8-8	The process owner must conduct a review at least once a year to ensure remote access and activity are appropriate and valid. Collected log data may be used in this review.
8-9	All inactive remote access accounts must be disabled as part of an unused account review.

8-10	The remote access service must be configured so that: a) remote access sessions are automatically disconnected after the predefined period of inactivity of 30 minutes b) remote access connections have an absolute connection time limit as defined by <organization name> c) remote access sessions use a <organization name> approved Virtual Private Network (VPN) connection d) remote users authenticate to the network using a <organization name> approved two-factor authentication (e.g. using their user ID and a hardware or software token) e) hardware or software tokens used for two-factor authentication must be uniquely associated with an individual use
8-11	<organization name> must implement organizational and technical controls to prohibit remote access for critical systems outside the Kingdom of Saudi Arabia.
8-12	All concurrent remote access (e.g., same user, multiple terminals) must be restricted and controlled.

Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>

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

3- **Standard Implementation and Execution:** <information technology function>

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

Update and Review

<cybersecurity function> must review the standard 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- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.

2- All personnel at <organization name> must comply with this standard.

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