4.7.1 Identity and Access Management (IAM)

Contents

Version	Adjustment Date	Approved By	Approval Date
2.0	4/7/2024	Saud Alsulami	7/7/2024

1. Definitions

For purposes of this “Identity and Access Management (IAM)” the following definitions apply:

- **Identity and Access Management (IAM):** A framework of policies and technologies for ensuring that the right individuals have the appropriate access to technology resources.
- **User Account:** A digital identity created for an individual user to access and use an organization's information systems.
- **Privileged Account:** An account that has more permissions than a standard user account, allowing it to perform administrative or specialized tasks.
- **Authentication:** The process of verifying the identity of a user or system
- **Authorization:** The process of granting or denying access to resources based on the identity of the user and their permissions
- **Multi-Factor Authentication (MFA):** A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity.
- **Least Privilege:** A security principle where users are granted the minimum levels of access – or permissions – needed to perform their job functions
- **Encryption:** The process of converting information or data into a code to prevent unauthorized access
- **Role-Based Access Control (RBAC):** A method of restricting system access to authorized users based on their roles within an organization

2. Purpose

The purpose of this policy is to establish guidelines for the management of user identities and access rights within Taqnyat. This ensures the security and integrity of our information systems by controlling and monitoring access to sensitive and critical information.

3. Scope

This policy applies to all employees, contractors, vendors, and any other individuals who have access to the Taqnyat information systems.

4. Policy

4.1. User Accounts and Privileged Accounts

- All users must have a unique user account.
- User accounts must be created, managed, and terminated by the NOC department.
- Privileged accounts must be strictly controlled and monitored.
- Use of privileged accounts must be limited to tasks that require elevated privileges.
- Privileged account access must be regularly reviewed.

4.2. Granting and Revoking Access Rights

- Access rights must be granted based on the principle of least privilege.
- Access requests must be approved by the asset owner and the IT department.
- Access to critical systems must require multi-factor authentication (MFA).
- Access rights must be revoked immediately upon termination of employment or contract.
- Regular audits must be conducted to identify and remove unnecessary access rights.

4.3. Authentication and Authorization Requirements

- All users must authenticate using a strong password and, where applicable, additional authentication methods.
- Authorization must be based on roles and responsibilities.
- All remote access must be logged and monitored.

4.4. Password Management Requirements

4.4.1. Active directory password:

- Passwords must meet complex requirements (minimum length 12-character, combination of letters, numbers, and special characters).
- Passwords must not be reused for at least 5 consecutive changes.
- Users must change their passwords every 90 days.
- System-enforced password changes must be implemented.
- Accounts must be locked after 5 failed login attempts.
- Locked accounts must be reviewed and unlocked by the NOC departments or systematically.

4.4.2. Taqnyat portal Password:

- Passwords must meet complex requirements (minimum length 8-character, combination of letters, numbers, and special characters).
- Passwords must not be reused for at least 5 consecutive changes.
- Users must change their passwords every 90 days.
- System-enforced password changes must be implemented.
- Accounts must be locked after 5 failed login attempts.
- Locked accounts must be reviewed and unlocked by the NOC departments or systematically.

4.5. Multi-Factor Authentication (MFA)

- MFA must be implemented for access to sensitive and critical information systems.
- MFA solutions must be approved by the NOC and cybersecurity department.
- For the Taqnyat's portal, user must add the IP address to whitelist before use it.

4.6. Access Rights Review

- User access rights must be reviewed every 6 months.
- Privileged access rights must be reviewed quarterly.
- Access rights to critical systems must be reviewed quarterly.

5. Non-compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

6. References

- ISO 27002
- SANS v7.0
- National Cybersecurity Authority's (NCA) ECC standards