Access

1. Purpose

An access policy defines the limitations and permissions to company information, information processing assets, and all other company resources. Standards, procedures, and controls provided here govern the management of user accounts, principles of Least Privileges, authentication and authorization, and logging of account actions.

2. Scope

The access policy is enforced for anyone who has been granted any kind of access to company network, resources, or both, including management, IT staff, third party employees, temporary employees, agents, vendors, and advisors.

3. Definitions

The Principle of Least privileged (PoLP) requires that access to systems, databases, information or any other specific resource should be restricted only to company roles that require them in order to perform their responsibilities.

4. User Account Management

User account management defines the registration of both existing and expired user accounts.

4.1 Establish an up-to-date user account inventory containing employee name, username, department, and dates activated.

4.2 Implement a secure employee account registration process.

4.3 Disable user accounts following termination, access rights revocation, or change in employee's position.

4.4 Remove inactive user accounts, preferably automatically.

4.5 Ensure that Default accounts of company assets are managed.

4.6 Establish a service account inventory containing service owner, review dates, and function.

4.7 Ensure that account identifiers are not reused within a predetermined period.

4.8 Secure and manage user account changes.

5. Authentication

Organizations must Authenticate, Authorize, and Audit (AAA) and uniquely identify organizational users and processes acting on behalf of organizational users.

5.1 Ensure that each user is assigned a unique identifier before being granted access to systems and services, avoiding the use of shared or generic accounts.

5.2 Enforce Multi-Factor Authentication for company assets and services that can be accessed from outside company network.

5.3 Enforce Multi-Factor Authentication for all privileged accounts for all company assets.

5.4 Ensure all applications are connected to a centralized Identity Provider (IdP).

5.5 Ensure that all account authentication is carried out using secure access protocols.

5.6 Blur feedback of authentication information.

5.7 Lock accounts that have exceeded predefined number of invalid login attempts.

5.8 Terminate idle remote sessions after a defined period of inactivity.

5.9 Verify that each privileged role only gets the minimum access permission needed.

5.10 Grant access rights and permissions based on role requirements.

6. User Account Access Management

Access rights and privileges are subjected to scrutiny and adjustments based on employee position or changes in company policies and regulations.

6.1 Use a central management system to manage account access to data and sensitive assets.

6.2 Establish a periodical audit of users' access rights and privileges.

6.3 Adjust users' access rights and privileges upon role changes.

6.4 Issue privacy and security notices to users upon logging into the organization system.

7. System and Application Access Control

System and application access controls define who might access systems and applications and under what terms.

7.1 Restrict access to information and application functions in accordance with the access-control policy.

7.2 Restrict the use of utility programs with system-overriding and application-control capabilities.

8. Detection of Unauthorized Access

Unauthorized access to company assets and resources can be prevented by applying tools and procedures to identify suspicious events and breaching attempts.

8.1 Log and monitor queries of company sensitive data.