**Access Control Policy**

Version:

Date:

Classification

Document Control

|  |  |  |
| --- | --- | --- |
| 1. | Document Title: |  |
| 2. | Date of Release: |  |
| 3. | Documents superseded: |  |
| 4. | Version No.: |  |
| 5. | Document Owner: |  |
| 6. | Document Author(s): |  |

Document Approvers

|  |  |  |  |
| --- | --- | --- | --- |
| S. No. | Approver | Approved Through Nominee | Nominee Contact |
|  |  |  |  |

Document Change Approvals

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Section / Page No. | Description of Amendment | Reason for Amendment | New Version No. and Effective Date | Amendment done by | Approved by |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Access Control Policy**

Access control policies provide the foundation for securing your data by providing effective access policies for your assets. Information Security Management System "ISMS" ISO 27001 compliance requires a comprehensive and detailed access control policy document covering all relevant areas of access control and permissions.

**Purpose**

Articulate the purpose of your acceptable controls policy. The primary purpose of the policy is to clearly establish asset access controls that include all systems and assets that contribute to the organization's critical functions. This includes PCs, networks, servers, and any kind of asset that can store and process data. The purpose of the policy is to protect employees and the organization. Organizations and employees are exposed to many types of risks when assets are not properly accessed and managed.

**Scope**

This policy applies to all employees, internal and external entities, suppliers and contractors.

**Access Control Policy:**

• Access to systems should be controlled and managed by access control rules defined for each system. must be included in the rule.

1. Physical and logical access controls (both)

2. Security requirements for each system. (Mainly critical systems)

3. Access control lists should be effectively implemented.

4. User rights should only be implemented by system administrators.

**Access to networks:**

• Access controls should be implemented such that any controls implemented meet all security requirements of the application.

• Monitor network usage.

• An authentication mechanism should be used to ensure that only authorized users can access the network.

• Properly implement firewall rules.

• Not all computers on the network have access to all available network resources. (Only necessary computers should be able to access necessary network resources.)

1. Make sure your security policies are updated.

2. Firewall security rules are clearly defined.

3. Use up-to-date antivirus software.

**User Access Provisioning:**

Whenever an authorized user accesses any kind of information object, this should be defined and documented. All approval processes should be tracked.

1. Approval Date

2.Approval Time.

3. List of permissions granted.

4. List of access rights.

5. Reason for access.

**User Access provisioning and revoking:**

• Get permission from your system administrator.

• Separation of duties to grant users only the privileges they need.

• Do not grant access until the authentication process is complete.

• Document all access rights for specific roles.

• Update and review access rights regularly and as needed.

• Access rights and privileges should be granted according to roles assigned to specific users.

• You should follow the principle of least privilege.

**Management of privileged access rights:**

• Identify and define the access rights and privileges required to complete each process.

• Identify and define the access rights and privileges required for each system.

• Grants the necessary access rights to complete the function.

• Consider system configuration options when providing access.

• User cannot access administrator and privileged accounts.

**Management of passwords:**

* For regular users, passwords must be at least 10 characters.
* System/IT administrator passwords must be at least 12 characters long.
* Passwords must contain at least two of the following items.

1. At least one lowercase letter [a – z]

2. At least one uppercase letter [A – Z]

3. At least one digit [0 – 9]

4. At least one special character [ @ ,#, %,^,& ,\*,!]

* Empty passwords are not allowed.
* Users must change their password immediately after logging in to their account for the first time.
* User accounts are locked for 10 minutes after 5 failed login attempts.
* Passwords must be changed at least every 60 days.
* A user cannot use the same password more than once when he changes his password.
* Each temporary password assigned by your company is only valid for a maximum of 6 hours.
* Passwords must be stored and transmitted using a cryptographic mechanism.
* IT entities must reset passwords upon valid request from a user.

**Review of User Access Rights:**

• If malicious activity is detected, the IT entity revokes or restricts all access rights.

• Please check your permissions.

1. Grant access to high-risk systems every two months.

2. Medium risk systems are granted access every six months.

3. Annual Access Rights for Low Risk Systems.

• Document all permissions granted to each role.

**Removal or adjustment of access rights:**

• Department Managers should notify as soon as possible if an employee changes an employee's role to HR.

• When an employee leaves the company, the following must be done.

1. You should notify your system administrator.

2. All access and privileges granted to the user must be terminated.

**Use of secret authentication information:**

• Users must be responsible for all activities related to the access granted.

• Users should not do this.

1. Give everyone the password over the phone.
   1. Show password in email.
   2. Talk to others about passwords.

IV. Reveal your password when completing forms and surveys.

1. Share your password with your family.

vi. Write the password on a piece of paper.

• The IT department must ensure that: a.

1. Passwords are encrypted at rest and in transit.
2. II. Passwords are not saved in Internet browsers.

**Password management system:**

• The IT department should be responsible for maintaining an effective password management system that ensures:

1. High-quality, unguessable passwords.
   1. Maintain a record of previously used passwords.
   2. Displays passwords as Asterix as they are typed.
   3. Separate password files from other application data files.
   4. Encrypt passwords during storage and transmission.
   5. Enforce periodic password changes when necessary.

**Use of privileged utility programs:**

• Users should not access system utilities unless they are authorized to do so.

• All access to system utilities should be tracked and logged.

• Unnecessary software should be uninstalled from the system.

**Access control to program source code:**

• Access to program source code is restricted to general users unless authorized.

• IT entities must ensure that all program source code is properly compiled and maintained.