**Access Control Policy**

**Access Control Policy**

The Access Control Policy lays the groundwork for data protection by establishing efficient access rules for the assets.

An Access Control Policy document that is thorough and extensive and that addresses all relevant aspects of access controls and privileges are required by the Information Security Management System (ISMS) as governed by ISO 27001.

**Purpose**

To express the Acceptable Control Policy's goal clearly. The policy's primary goal is to define access restrictions for all systems and assets, particularly those that support the crucial operations of the company. Personal computers, networks, servers, and any other type of asset that can store and process data are included in this. The policy's protection of the organization's workers is its main objective. The organization and the employees would be exposed to many types of dangers if assets are not effectively accessible and managed.

**Scope**

All workers, internal entities, external entities, suppliers, and contractors are subject to this policy.

**Access Control Policy:**

* Access control rules that are specifically specified for each system should be used to manage and regulate access to the systems. The guidelines should include.

1. Logical and physical access restrictions (Both)
2. Specifications for each system's security. (Most often the crucial systems)
3. Access control lists should be adequately established.
4. The system administrator should be the sole one to implement user permissions.

**Access to networks:**

* When implementing access controls, care should be taken to ensure that each control complies with the application's security needs.
* Keep an eye on network usage.
* To ensure that only authorized users can access networks, authorization techniques should be used.
* Correctly apply the firewall rules.
* Not every machine connected to a network should have access to every network resource. Make sure that (only the necessary machines should have access to the necessary network resources).

1. Security guidelines have been modified.
2. Clearly stated firewall security rules.
3. Use antivirus software that is up to date.

**User Access Provisioning:**

* Any time a legitimate user accesses a certain information asset, it needs to be specified and recorded. All permission procedures must be monitored.

1. Date of Authorization II. Time of Authorization
2. A list of the access rights given.
3. IV. The list of access privileges
4. V. The justification for access.

**User Access provisioning and revoking:**

* Getting permission from the system administrator.
* Segregation of duties to guarantee that a user only receives the necessary privileges.
* Before to the authorization procedure is finished, access permissions should not be granted.
* Lists all the access privileges for a specific position.
* Update and check the access rights as needed and regularly.
* Access rights and privileges ought to be granted by the role that has been given to a certain user.
* Should adhere to the least access, greatest responsibility rule.

**Management of privileged access rights:**

* Identify and provide the privileges and access rights needed to accomplish each process.
* Identify and specify the privileges and access rights needed for each system.
* Grant the necessary access privileges to carry out the necessary tasks.
* Take into account system configuration capabilities when granting access rights.
* Privilege and admin accounts shouldn't be accessible to users.

**Management of passwords:**

* For typical users, the password should contain at least 10 characters.
* Passwords for system/IT administrators must include at least 12 characters.
* At least two of the following should be included in the password.

1. One or more lowercase letters (a–z)
2. A minimum of one uppercase letter (A–Z)
3. At least one digit (0–9)
4. At least one special character [@,#,%,,&,\*,!] must be used.

* No blank passwords are permitted.
* After logging into an account for the first time, users should promptly change their password.
* After five failed login attempts, the user's account will be locked for 10 minutes.
* A new password needs to be set at least every 60 days.
* When changing passwords, users are not permitted to use the same password more than once.
* The company will only issue temporary passwords that are good for a maximum of six hours.
* Passwords should be transferred and stored using encryption techniques.
* Upon receiving a legitimate request from the user, the IT unit must reset the password.

**Review of User Access Rights:**

* Ifat harmful activity is discovered, the IT unit must revoke or restrict any access rights.
* Examine the rights of access.

1. High-risk systems receive access rights every two months.
2. Medium-risk systems receive access rights every six months.
3. Every year, access privileges are granted for low-risk systems.

* Keep a record of every access privilege granted for each role

.**Removal or adjustment of access rights:**

* The department manager should notify HR as soon as possible if any employee changes their employee role.
* Should do the following whenever an employee quits or is fired from their position.

1. The system administrators need to be informed.
2. The user should lose all access and privileges that have been granted to them.

**Use of secret authentication information:**

* Users must take responsibility and accountability for all actions relating to the access rights granted to them.

1. Tell anyone over the phone the password.
2. Email yourself the password.
3. Discuss passwords with others.
4. When completing forms and questionnaires, reveal passwords.
5. Password-sharing among family members.
6. Write passwords on paper in item six.

* The IT department should make sure that:

1. Passwords are encrypted while being stored and transported.
2. Internet browsers do not save passwords.

**Password management system:**

* The IT unit should be in charge of upholding a strong password management system that guarantees:

1. Strong, impenetrable passwords.
2. Keep track of passwords that have already been used.
3. When typing, passwords are displayed as Asterix.
4. Password files and other application data files should be kept apart.
5. Encrypt passwords while they are being stored and sent.
6. When necessary, enforce routine password changes.

* Application of privileged utility software

1. Users shouldn't access system utilities unless they have permission to.
2. All system utility access should be monitored and recorded.
3. The system should be cleared of any extraneous software.

**Access control to program source code:**

* Regular users cannot view program source codes unless they have permission to do so.
* The IT department should make sure that all program source codes are correctly preserved and assembled.