**Access Management Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_9v9b9bt91r7c) **4**

[**Scope**](#_hifuy8vpzt2a) **4**

[**Policy**](#_yzpsqigj3sk) **4**

[**Account Types**](#_9df6qij95c0) **4**

[**Privileged Accounts**](#_4fythr65zkrp) **4**

[**Default User Accounts**](#_v2ecnfm79i5q) **5**

[**Test Accounts**](#_tivnd6rkrhri) **5**

[**User Registration**](#_812y2rg3q6n9) **5**

[**Account De-Registration**](#_9f8zdn4xw05s) **5**

[**Management of Privileged Accounts**](#_hx62s24botiv) **5**

[**Third-Party Access**](#_ovuw7h8afzg8) **6**

[**Access Rights Review**](#_jil84ki6u7h0) **6**

[**Password Management**](#_t2do2uq2je9q) **6**

[**Strong Passwords**](#_gkph78l7hbta) **6**

[**Weak Passwords**](#_vmwdqdu3i96n) **6**

[**Password Confidentiality**](#_llwi1sqffq3b) **7**

[**Password Uniqueness**](#_u1ff95eqhv2c) **7**

[**Password Change Frequency**](#_n3ehzhjwab6e) **7**

[**Change, Review, and Update**](#_w1o88vxspwq8) **7**

[**Disciplinary Action**](#_1b64a7ktf8py) **8**

[**Responsibility**](#_3z6f7qtfare9) **8**

[**Related Documents**](#_pgexw9pbtts8) **8**

# 

# **Purpose**

This policy aims to describe the processes in the company regarding access management, starting from access granting to access revoking. Also, this policy must ensure that users have the appropriate access levels to sensitive data and systems.

# **Scope**

This policy covers access to all business processes and data, systems, and other IT resources owned or operated by *[Company]*.

This policy applies to all employees, whether employed full-time or part-time, contractors, subcontractors, and third parties.

# **Policy**

* All *[Company]* IT resources must be password protected.
* Access to the *[Company]* information systems must be strictly controlled by formal registration and de-registration process.
* Each *[Company]* information system must have a designated system owner responsible for managing and controlling access to the system.
* Access to *[Company]* information systems must be controlled by using individual user accounts.
* *[Company]* will provide access to the company’s systems on the following principles:
  + **Need to know** – users or resources will be granted access to systems necessary to fulfill their roles and responsibilities.
  + **Least privilege** – users or resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.

## **Account Types**

### **Privileged Accounts**

* Privileged user accounts can only be requested by managers or supervisors and must be appropriately approved.

### **Default User Accounts**

* Where possible, all default user accounts will be disabled or changed. These accounts include “guest,” “temp,” “admin,” etc.

### **Test Accounts**

* Test accounts can only be created if justified by the relevant business area or project team and approved by the application owner through a formal request. The IT Manager should approve the request.
* Test accounts should be disabled/deleted when they are no longer necessary.
* The credentials for test accounts can be shared between the employees only if testing procedures require using those credentials.

## **User Registration**

* All user IDs on *[Company]’s* systems should be constructed according to the one approved company’s user ID construction standard, must indicate the responsible individual’s name.
* Every user should have a single unique user ID and a password for access.
* The MFA usage should be enabled whenever it is possible.
* Using an old user ID or terminated employee user ID from the company is unacceptable.
* Usage of one user ID by two different employees is unacceptable.
* Self-provision of the credentials to another employee or person who is not working in *[Company]* is unacceptable.
* System Administrator creates new user accounts only after receiving the request.

## **Account De-Registration**

* As soon as a user leaves the employment of *[Company]*, all his/her information systems access accounts must be revoked immediately.

## **Management of Privileged Accounts**

* Privileged access to *[Company]* systems must be allocated based on the user’s functions.
* The principle of least privilege must be followed when granting privileged rights.
* Access privileges granted to users must not undermine essential segregation of duties.
* The creation of user access accounts with special privileges such as administrators must be controlled and restricted to only those responsible for managing or maintaining the information systems.

## **Third-Party Access**

* Third parties will have a legitimate business need for access to the company’s systems. When such need is demonstrated, temporary guest access to company systems is permitted.
* This access must be severely restricted to only those resources that the third party needs at that time and disabled when the guest’s work is completed.

## **Access Rights Review**

* The system owner must conduct a quarterly review of the access rights. Any violations found should be addressed in the shortest time possible.
* *[Company]* performs a quarterly review of Amazon Security Group rules. This quarterly review includes base configuration, administrative access, monitoring, and security settings.

## **Password Management**

### **Strong Passwords**

* The password contains both upper- and lower-case characters (e.g., a-z, A-Z).
* The password has digits and punctuation characters as well as letters, if possible (e.g. 0-9, !@#$%^&\*()\_+|~-=\`{}[]:";'<>?,./).
* The password is at least fourteen (14) alphanumeric characters long.
* The password is not a word in any language, slang, dialect, jargon, etc.
* The password is not based on personal information, names of family, etc.

### **Weak Passwords**

* The password contains less than fourteen (14) characters.
* The password is a word found in the English or foreign dictionary.
* The password is a common usage word, such as:
  + Company-related information.
  + Names of family members, pets, friends, co-workers, fictional characters, etc.
  + Computer terms and names, commands, sites, companies, hardware, and software terms.
  + Birthdays and other personal information, such as addresses and phone numbers.
  + Word or number patterns like aaabbb, qwerty, xyzzy, 123321, etc.
  + Any of the above spelled backward.
  + Any of the above preceded or followed by a digit (e.g., secret1, 1secret, etc.).

### **Password Confidentiality**

* Employees must not disclose their passwords to anyone.
* Employees must not share their passwords with others (co-workers, supervisors, family, etc.).
* Employees must not write down their passwords and leave them unsecured.
* Employees must not check the "save password" box when authenticating to applications.
* Employees must not use the same password for different systems and accounts.
* Employees must not reuse passwords.
* Employees can use an approved password manager for password storing to remember only the master password to access that DB.
* Employees must lock their laptops when inactive and re-enter the password.

### **Password Uniqueness**

* User accounts with system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
* Users are not allowed to use the same password to access multiple company systems.

### **Password Change Frequency**

* Passwords should be periodically changed. At a minimum, users must change passwords every 90 days.

# **Change, Review, and Update**

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by IT Manager.

# **Disciplinary Action**

Employees who violate this policy may face disciplinary consequences in proportion to their violation. *[Company]’s* management will determine how severe an employee’s offense is and take the appropriate action.

# **Responsibility**

The IT Manager is responsible for ensuring this policy is followed.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related Documents**

* Asset Management Policy
* Supply Chain and Business Partner Policy