*Account Management Policy*

Table of Contents

[Purpose 1](#_Toc5046274)

[Scope 1](#_Toc5046275)

[Policy 1](#_Toc5046276)

[System Authorization 1](#_Toc5046277)

[Account Categorization 2](#_Toc5046278)

[Account Definition 2](#_Toc5046279)

[Separate of Duties 2](#_Toc5046280)

[Duration Setting 3](#_Toc5046281)

[Account Maintenance 3](#_Toc5046282)

[Administrator and Privileged Accounts 3](#_Toc5046283)

[Privileged Account Management 3](#_Toc5046284)

[Violations 4](#_Toc5046285)

[Definitions 4](#_Toc5046286)

[References 5](#_Toc5046287)

[Related Documents 5](#_Toc5046288)

[Approval and Ownership 5](#_Toc5046289)

[Revision History 5](#_Toc5046290)

Purpose

This policy defines the control requirements for the secure management of accounts on CompanyX (the “Company”) Information systems.

Scope

This policy applies to all CompanyX computer systems and facilities, with a target audience of CompanyX Information Technology employees and partners.

(Note: This policy provides more granular controls than those provided in Access Control Policy.)

Policy

### System Authorization

**Identification For System Usage -** All users must be positively identified prior to being able to use any information system resources.

**Unique User ID And Password Required** - Every user must have a single unique user ID and a personal secret password for access to CompanyX information systems.

**User ID Authorization** – Requests for the addition, deletion, and modification of all user IDs, credentials, and other identifier objects on CompanyX information systems must be submitted on a form (or electronically) authorized by the worker's immediate supervisor or manager.

### Account Categorization

**Account Categorization** – All accounts created on CompanyX systems must fall into one of three categories, each designed for different levels of control and security. Accounts and corresponding passwords must fall into the following two categories:

* **User Account (Identity)** – This account may represent a human being and therefore that password determines identity e.g. an active directory user account – the password on the account is the secret known by the human that identifies that human to the system. An identity password should not be associated with a privileged account but rather a regular user account.
* **Privileged (Identity) Account** – Privileged accounts are associated with a specific human being, but these accounts have expanded privileges in order to maintain systems. Examples include system administrator accounts. These accounts must be limited, and the passwords can be set to larger values and perhaps stored in the privileged account management system.
* **System (Non-Identity) Account** – Non-identity accounts are not associated with a specific human being, but a system or service (for example system account like UNIX root or a service account) The passwords on these accounts do not provide for any identity of a human and therefore do not need to be memorized. These passwords can be set to very large values and stored in the privileged account management system.

### ****Account Definition****

**Unique User IDs** - Each information system account user ID must uniquely identify only one user. Shared or group user IDs must not be created or used.

**User ID Construction**- All user IDs on CompanyX information systems must be constructed according to the CompanyX user ID construction standard, must clearly indicate the responsible individual’s name.

**Generic User IDs** - User IDs must uniquely identify specific individuals and generic user IDs based on job function, organizational title or role, descriptive of a project, or anonymous, must not be created or used.

**Re-Use Of User IDs** - Each CompanyX information system user ID must be unique, connected solely with the user to whom it was assigned, and must not be reassigned after a worker or customer terminates their relationship with CompanyX.

**Role-Based Password Length - The minimum length for fixed passwords must be set to six for handheld computers, eight for all network-connected computers, and ten for administrator and other privileged user IDs.**

### ****Separate of Duties****

**Systems Administrator User IDs** - System administrators managing computer systems with more than one user must have at least two user IDs, one that provides privileged access and is logged, and the other that provides the privileges of a normal user for day-to-day work.

### ****Duration Setting****

**User ID Expiration** - Expiration dates must be set for all user IDs on CompanyX information systems. When user IDs expire, privileges for user IDs must be automatically be revoked, and the files linked to these user IDs must be retained for at least a two-week period.

**User ID Expiration Period** - User IDs on Internet-accessible computers must be set to expire six months from the time they are established and renewable in six-month intervals.

**Third Party User ID Expiration** - Every user ID established for a third-party (non-employee) must have a specified expiration date, with a default expiration of 30 days when the actual expiration date is unknown.

### Account Maintenance

**User Status Changes** - Every change in the status of a User that would change their access to information or systems must be reported to the Information Technology Department.

**Inactive Account Maintenance** - All inactive accounts over 90 days old must be either removed or disabled.

### Administrator and Privileged Accounts

**Privileged User Account Approval** – The creation or modification of privileged user accounts must be approved by at least two individuals: The System Owner and an authorized member of the Information Technology department. System administrators must not be allowed to create other privileged accounts without authorization.

**Number Of Privileged User IDs** - The number of privileged user IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes.

**Privileged Account Requirements** – All privileged accounts on CompanyX systems must employ greater security than non-privileged accounts. This includes longer, more secure passwords and greater audit accountability.

**Role Based Account Privileges** – To facilitate secure management of systems, wherever possible, privileged accounts must be defined based on the specific role of the system administrator.

### Privileged Account Management

**Privileged Account Inventory** – CompanyX must maintain an inventory of all accounts with privileged access on production information systems. These include, at a minimum, local administrator accounts and service accounts.

**Central Automated Management** – All privileged accounts on CompanyX systems must be managed by a central system. This system must provide an audit trial that tracks specific additions, changes and deletions.

**Integration with Native Directories** – Any privileged account management system must integrate with native operating system account management systems or directory services (such as Active Directory)

**Integration with Strong Authentication Methods** – Any privileged account management system must integrate with strong authentication methods (such as two factor authentication) to ensure the identity of the user in addition to their directory authentication.

**Password Vault** – CompanyX system administrators must have access to a vault system which enables the temporary provisioning of access to privileged accounts and passwords (aka FireID) for emergency maintenance.

**Password Vault Encryption – CompanyX must maintain any credentials stored in a central management system within an encrypted password vault, using strong encryption algorithms that meet compliance and/or regulatory requirements.**

**Account Inventory Update** – The privileged account inventory must be updated at least quarterly to identify new or changed accounts.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. CompanyX reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. CompanyX does not consider conduct in violation of this policy to be within an employee’s or Third-Party’s course and scope of employment, or the direct consequence of the discharge of the employee’s or Third-Party’s duties. Accordingly, to the extent permitted by law, CompanyX reserves the right not to defend or pay any damages awarded against employees or Third-Parties that result from violation of this policy.

Any employee or Third-Party who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Definitions

**Account (User ID or Username)** - A unique string of characters assigned to a user by which a person is identified to an Information system or network. A user commonly must enter both a user ID and a password as an authentication mechanism during the logon process.

**Information System** – Any multi-user computer or communications system resource, including network devices, servers, or applications. These include third-party hosted services that provide production support to CompanyX operations.

**Password** **–** An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

**Privileged Account** **–** Any system account that has privileges beyond standard User accounts. Examples include Administrator accounts, system accounts and Unix “Root” accounts.

**System Administrator –** An employee or Third-Party who is responsible for managing a CompanyX multi-user computing environment. The responsibilities of the system administrator typically include installing and configuring system hardware and software, establishing and managing user accounts, upgrading software and backup and recovery tasks.

**Third-Party –** Any non-employee of CompanyX who is contractually bound to provide some form of service to CompanyX.

**User -** Any CompanyX employee or Third-Party who has been authorized to access any CompanyX electronic information resource.

References

ISO/IEC 27002 - 9.2.1 User registration and de-registration

NIST: Identification and Authentication (IA)

PCI-DSS: 8.1 User ID Management

US-CSF: PR.AC-1: Identities and credentials are managed for authorized devices and users

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | 10/05/2019 | MM/DD/YYYY |  |
|  |  |  |  |  |