*Access Control Policy*

Table of Contents

[Purpose 1](#_Toc3901605)

[Scope 1](#_Toc3901606)

[Policy 1](#_Toc3901607)

[Access Restrictions 1](#_Toc3901608)

[User ID and Account Management 1](#_Toc3901609)

[Access Authorization 2](#_Toc3901610)

[Password Requirements 2](#_Toc3901611)

[System Privileges 2](#_Toc3901612)

[Session Controls 3](#_Toc3901613)

[System Authentication 3](#_Toc3901614)

[Records 3](#_Toc3901615)

[Access Review 4](#_Toc3901616)

[Violations 4](#_Toc3901617)

[Definitions 4](#_Toc3901618)

[References 5](#_Toc3901619)

[Related Documents 5](#_Toc3901620)

[Approval and Ownership 5](#_Toc3901621)

[Revision History 5](#_Toc3901622)

Purpose

This policy defines the requirements for secure access to CompanyX (the “Company”) Information systems.

Scope

This policy applies to all users of CompanyX information assets including but not limited to CompanyX employees and Third-Parties.

Policy

### Access Restrictions

**Access Control Systems** - All CompanyX technology platforms (i.e. network, operating system, application, and database) must authenticate the identity of users (including other systems accessing these platforms) using unique user IDs and passwords.

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

### User ID and Account Management

(Note: The Account Management Policy provides a more detailed list of user account management controls.)

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

**Generic User IDs** - User IDs must uniquely identify specific individuals and generic user IDs based on job function must not be created or used.

**Reuse 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.

**User ID Expiration** - - Expiration dates must be set for all user IDs on multi-user systems at CompanyX. 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.

### Access Authorization

**Access Control 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 authorized by the worker's immediate supervisor or manager.

**Evidence Of User Agreement** - Before they are granted access to CompanyX information systems, all users must provide documented evidence of their agreement to comply with CompanyX information security and privacy requirements.

**Sensitive Information Access** - Access to CompanyX sensitive information must be provided only after express management authorization has been obtained from the designated owner of such information.

### ****Password Requirements****

**Minimum Password Length - All passwords must have at least 8 characters and this length must always be checked automatically at the time that users construct or select their password.**

**Password Complexity - All user-chosen passwords must contain at least one alphabetic and one non-alphabetic character.**

**Null Passwords Always Prohibited** - At no time, may any Systems Administrator or Security Administrator enable any user ID that permits password length to be zero (a null or blank password).

**Password Change Requirements - All users must be automatically required to change their passwords at least once every 90 days.**

**Password History - On all multi-user CompanyX computers, system software or locally-developed software must be used to maintain an encrypted history of previously chosen fixed passwords. This history must contain at least the previous thirteen passwords for each user ID.**

### System Privileges

**Privilege Restriction - Need To Know** - The **Information** system privileges of all users, systems, and programs must be restricted based on the need to know.

**Special Privileged Users** - All multi-user computer and network systems must support a special type of user ID, which has broadly-defined system privileges that will enable authorized individuals to change the security state of systems.

**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.

### ****Session Controls****

**Session Timeout** – Access control systems must be configured to automatically logoff users after a period of inactivity of 15 minutes.

**Maximum Logon Attempts – Access control systems must be configured to automatically disable User IDs after six unsuccessful logon attempts.**

**Account Lockout Duration – All user IDs that have been locked out or disabled must remain locked for a period of at least 30 minutes.**

**Incorrect Logon Information -** When logging on to a CompanyX **Information** system, if any part of the logon sequence is incorrect, the system must terminate the session and wait for the correct logon information. Prompts or feedback to the user, of any form and of any nature, is prohibited.

### System Authentication

**System Logon Banner -** Every logon screen for multi -user computers must include a special notice which must states that the system may only be accessed by authorized users, users who logon represent that they are authorized to do so, unauthorized system usage or abuse is subject to criminal prosecution, and system usage will be monitored and logged.

**Last Logon Notice -** At logon time, every user must be given information reflecting the last logon time and date.

**Daily Logon Limits -** Users must not be permitted to log on more than 10 times a day.

### Records

**Access Control System Logging** - Access control systems must be configured to capture and maintain the following:

* The creation date for every user ID.
* Date and time of the last logon for every user ID.
* Date and time of the last logoff for every user ID.
* Date and time of the last password change for every user ID.
* An expiration date or every user ID that represents the last date that the user ID is active for use.
* Details of addition and changes to the privileges of user IDs.

**Access Control Privilege Log Retention** - Computerized records reflecting the access privileges of each user of CompanyX multi-user systems and networks must be securely maintained for at least 90 days.

**User ID Records** - Records reflecting all the Information systems on which users have user IDs must be kept current.

### Access Review

**Reauthorization Of User Access Privileges** - The system privileges granted to every user must be reevaluated by the user’s immediate manager annually to determine whether currently-enabled system privileges are needed to perform the user’s current job duties.

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

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 contractor 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 a Information system or network. A user commonly must enter both a user ID and a password as an authentication mechanism during the logon process.

**Confidential Information (Sensitive Information)** – Any CompanyX information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by CompanyX from a Third-Party under a non-disclosure agreement.

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

**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.

**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.

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

References

ISO/IEC 27002 – 9.0 Access Control

NIST: Access Control (AC)

PCI-DSS: R7. Restrict access to cardholder data by business need to know

US-CSF: PR.AC Access Control

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 |  |
|  |  |  |  |  |