*Physical Security*

*Policy*

Table of Contents

[Purpose 1](#_Toc3894090)

[Scope 1](#_Toc3894091)

[Policy 1](#_Toc3894092)

[Physical Security Perimeter 1](#_Toc3894093)

[Physical Access Control 1](#_Toc3894094)

[Access Control Monitoring 2](#_Toc3894095)

[Physical Access Authorization 2](#_Toc3894096)

[Access Badges 2](#_Toc3894097)

[Visitor Handling 3](#_Toc3894098)

[Access Review 3](#_Toc3894099)

[Access Testing 3](#_Toc3894100)

[Violations 4](#_Toc3894101)

[Definitions 4](#_Toc3894102)

[References 4](#_Toc3894103)

[Related Documents 4](#_Toc3894104)

[Approval and Ownership 4](#_Toc3894105)

[Revision History 5](#_Toc3894106)

Purpose

This policy defines the requirements for establishing physical access controls at CompanyX (the “Company”) locations.

Scope

This policy applies to all CompanyX facilities, with a target audience of all employees and Third-Parties.

Policy

### ****Physical Security Perimeter****

Security Perimeter - Access to every CompanyX secure area must be controlled by a clearly defined security perimeter.

### ****Physical Access Control****

**Physical Access Control To Sensitive Information** - Access to every work area containing sensitive information must be physically restricted to limit access to those with a need to know.

Guarded Access - All Third-Party access to CompanyX offices, computer facilities, and other work areas containing sensitive information must be controlled by guards, receptionists, or other staff.

**Unauthorized Physical Access Attempts** - Workers must not attempt to enter restricted areas in CompanyX buildings for which they have not received access authorization.

**Terminated Worker Access To Restricted Areas** - Whenever a worker terminates his or her working relationship with CompanyX, all access rights to CompanyX restricted areas must be immediately revoked.

**Restricted Area Working Hours** - Authorized workers must not access restricted CompanyX facilities where sensitive, critical, or valuable information is handled at any time other than authorized access hours.

### Access Control Monitoring

**Access Control System Records** - The Security Department must maintain records of the persons currently and previously inside CompanyX buildings and securely retain this information for at least three months.

**Physical Access Monitoring - Method** - Video cameras or other access control mechanisms that monitor the entry and exit points to secure areas must be in place.

**Physical Access Monitoring - Security** - Video cameras or other access control mechanisms that monitor secure areas must be protected from tampering and disabling.

### Physical Access Authorization

**Physical Access Badge Procedures** - Procedures must be developed and implemented that control the issuance, modification, and revocation of CompanyX physical access badges.

**Physical Access Badge System Access** - Access to the system that controls the CompanyX physical access badges must be limited to only those employees with the responsibility to issue, modify, or revoke physical access badges.

### Access Badges

**Badge-Controlled Access** - Each person must present his or her badge to the badge reader before entering every controlled door within CompanyX premises.

**Identification Badges** - When in CompanyX secure buildings or facilities, all persons must wear an identification badge on their outer garments so that both the picture and information on the badge are clearly visible to all people with whom the wearer converses.

**Securing Identification Badges** - When off CompanyX premises, workers must protect their identification badges with the same level of protection as their wallets and credit cards.

**Removing Identification Badges** - Immediately after workers leave CompanyX facilities, they must remove their identification badges and store them in a safe and convenient place away from public view.

**Temporary Badges** - Workers who have forgotten their identification badge must obtain a one-day temporary badge by providing a driver’s license or another piece of picture identification.

**Badge Access Sharing** - Workers must not permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when authorized persons go through these entrances.

**Individuals Without Identification Badges** - Individuals without a proper CompanyX identification badge in a clearly visible place must be immediately questioned about their badge and if they cannot promptly produce a valid badge, they must be escorted to the receptionist desk.

### ****Visitor Handling****

**Visitor Identification** - All visitors to CompanyX must show picture identification and sign a log prior to gaining access to restricted areas.

**Escorting Visitors** - Visitors to CompanyX offices including, but not limited to, customers, former employees, worker family members, equipment repair contractors, package delivery company staff, and police officers, must be escorted at all times by an authorized worker.

**Visitor Badge - Identification** - All visitors must be provided with a badge that clearly identifies them as a non-employee.

**Visitor Badge - Expiration** - All visitor badges must be set to expire no longer than the end of the current day.

**Visitor Badge - Surrender** - All visitors must surrender their badge to the issuing party or their employee escort before leaving any CompanyX facility.

**Visitor Log - Contents** - A visitor log must be maintained that contains the visitor's name, the firm represented, and the employee authorizing physical access to any CompanyX facility.

**Visitor Log - Retention** - Visitor logs must be retained for at least three months.

**Unescorted Visitors** - Whenever a worker notices an unescorted visitor inside CompanyX restricted areas, the visitor must be questioned about the purpose for being in restricted areas, then be accompanied to a reception desk, a guard station, or the person they came to see.

### ****Access Review****

**Physical Access Monitoring - Data Review** - The data that is produced by video cameras or other access control mechanisms that monitor the entry and exit points to secure areas must be monitored.

### ****Access Testing****

**Testing of Physical Security Perimeter** - CompanyX will perform a comprehensive testing of the physical security controls of each location at least annually.  This testing includes at the minimum physical access controls, physical access monitoring controls and logging controls.

**Third-Party Physical Penetration Testing Required** - CompanyX must hire a qualified, independent Third-Party to conduct a physical security penetration test at least once a year.

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

**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.

**Visitor** -Any person who does not normally work in a CompanyX facility or who does not perform regular business functions requiring access to or entry into a CompanyX facility.

References

ISO/IEC 27002: 11.1 Secure Areas

NIST: Physical and Environmental Protection (PE)

PCI-DSS: R9. Restrict physical access to cardholder data

US-CSF: PR.AC-2: Physical access to resources is managed and secured

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 |  |
|  |  |  |  |  |