Physical Security Policy

Document Classification:	
Document Ref.	
Version:	**1**
Date:	
Document Author:	
Document Owner:	

Revision History

Version	Date	Revision Author	Summary of Changes

Distribution

Name	Title

Approval

Name	Position	Signature	Date

Purpose

This policy defines the requirements for establishing physical access controls at $Company$ locations.

Scope

This policy applies to all $Company$ facilities, with a target audience of all employees and partners.

Policy

Access Control

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

Access To Computers and Communications Systems - Buildings that house $Company$ computers or communications systems must be protected with physical security measures that prevent unauthorized persons from gaining access.

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

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

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

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

Access Control Monitoring

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 Badge Procedures - Procedures must be developed and implemented that control the issuance, modification, and revocation of $Company$ physical access badges.

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

Securing Propped-Open Computer Center Doors - Whenever doors to the computer center are propped-open, the entrance must be continuously monitored by an employee or a contract guard from the Physical Security Department.

Access Badges

Identification Badges - When in $Company$ 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 $Company$ 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 $Company$ 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-Controlled Access - Each person must present his or her badge to the badge reader before entering every controlled door within $Company$ premises.

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 $Company$ 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.

Visitors

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

Third-Party Physical Access - Visitor or other third-party access to $Company$ offices, computer facilities, and other work areas containing sensitive information must be controlled by guards, receptionists, or other staff.

Escorting Visitors - Visitors to $Company$ 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.

Escorts Required For All After-Hour Visitors - Visitors must be escorted by an employee authorized by a department manager whenever they are in $Company$ offices or facilities outside of normal business hours.

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 $Company$ 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 $Company$ facility.

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

Third-Party Supervision - Individuals who are neither $Company$ employees, nor authorized contractors, nor authorized consultants, must be supervised whenever they are in restricted areas containing sensitive information.

Repair People Who Show Up Without Being Called - Every third party repair person or maintenance person who shows up at $Company$ facilities without being called by an employee must be denied access to the facilities. All such incidents must be promptly reported to the Information Security Department.

Unescorted Visitors - Whenever a worker notices an unescorted visitor inside $Company$ 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.
Data Center And Information Systems Department Visitors - Visitors who do not need to perform maintenance on $Company$ equipment, or who do not absolutely need to be inside the Data Center or Information Systems Department, must not enter these areas.

Computer Facility Tours - Public tours of $Company$'s major computer and communications facilities must never be conducted.

Access Review

Computer Center Staff Access - A complete list of all workers who are currently authorized to access the computer center must be maintained, reviewed, and updated by the Computer Operations Manager on a quarterly basis.

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.

Testing

Testing of Physical Security Perimeter - $Company$ 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 - $Company$ 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. $Company$ reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. $Company$ does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, $Company$ reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner 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.