# Physical Protection Procedure

|  |  |  |  |
| --- | --- | --- | --- |
| Procedure Owner |  |  | |
| Procedure Approver(s) |  |
| Effective Date |  | Next Review Date |  |

# Purpose

The purpose of this procedure is to define a consistent approach to manage Physical Protection of the IT environment at [COMPANY NAME].

# Scope

This procedure is consistent with CMMC and covers all network and system access procedures within [COMPANY NAME] environment. This procedure will be followed by all employees of [COMPANY NAME]. The CMMC System Security Plan (SSP) will be updated to reflect any significant modifications made to this procedure.

# Definitions

**Employees**: All individuals belonging to one or many groups defined below:

1. All individuals associated with [COMPANY NAME] through an employee – employer relationship or contract between [COMPANY NAME] and their employer or [COMPANY NAME] and individual.
2. All individuals possessing equipment issued by [COMPANY NAME]
3. All individuals working on the premises of [COMPANY NAME] and/or utilizing the Internet services provided by [COMPANY NAME].

# Governing Laws, Regulations, and Policies

* NIST SP 800-171, 3.10.1 - 3.10.6
* CMMC PE.L1-3.10.1 – PE.L2-3.10.6
* [COMPANY NAME] – PE – 3.10 - Physical Protection Policy

# Procedure Statements

**PE.L1-3.10.1 – Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals:**

1. [COMPANY NAME] limits physical access to organizational information systems, equipment, and the respective operating environment to authorized individuals. This applies to employees, individuals with permanent physical access authorization credentials and visitors.
2. Limiting physical access to organizational systems includes placing organizational information systems in secured areas and allowing access to authorized individuals only and placing organizational information systems in locations that can be monitored by organizational personnel.
3. Limiting physical access to equipment includes placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.
4. [COMPANY NAME] manages all in/out-processing procedures through <Human Resources>. Through these procedures, <FSO> issues authorization credentials for physical access to [COMPANY NAME] Operating Environments and maintains a list of authorized personnel. A completed and approved System Authorization Access Request (SAAR), Non-disclosure Agreement (NDA), and Proximity badge, are required before any personnel are granted access to facilities. Physical access to facilities where the information system (IS) resides is based on position or role. <FSO> reviews the access list which details facility access by authorized personnel monthly. When an individual no longer requires access (for any reason) to [COMPANY NAME] facilities, they are immediately removed from the list of authorized personnel by the <FSO>.

**PE.L1-3.10.3 – Escort visitors and monitor visitor activity:**

1. All visitors to [COMPANY NAME] facilities shall be required to establish proper company sponsorship, furnish appropriate identification, indicate citizenship status, and register before admittance to the facilities. An [COMPANY NAME] employee (i.e. no contractor escort) must escort any authorized visitors accessing [COMPANY NAME] facilities. There are no areas within any [COMPANY NAME] facilities that are deemed publicly accessible other than the front lobby of the facility. There are also security cameras located throughout interior and exterior of the facility. Access to physical locations is enforced by:

* Ensuring the individual requesting access is whom they claim to be before granting access to the facility.
* Controlling ingress and egress points to the facility using physical access locking mechanisms.
* Any visitors not otherwise permitted unescorted access are required to be escorted and monitored at all times

1. In addition, facilities and offices monitor visitor activity and escort visitors at all times. Visitors wear special visitor badges while on the property. A Visitor’s log is maintained. The visitor’s log is a written log of individuals accessing the facility, automated visitors log that captures ID, or some combination thereof.

**PE.L1-3.10.4 – Maintain audit logs of physical access:**

1. <FSO> issues authorization credentials for physical access to [COMPANY NAME] facilities and maintains a list of authorized personnel. Physical access devices include keys, locks, combinations, or card or badge readers. The list of Authorized personnel is reviewed every 30 days and maintained for a period of one year. [COMPANY NAME] maintains audit logs produced by the physical access control system and the <front lobby personnel> for visitor access. Visitor access records are reviewed every 30 days and maintained for a period of one year. [COMPANY NAME] employs automated mechanisms such as [please list automated mechanisms for log monitoring such as the badging system] to facilitate the maintenance and review of access records. Additional information on visitors can be location in the Visitor Access Control Policy.

**PE.L1-3.10.5 – Control and manage physical access devices:**

1. [COMPANY NAME] controls and manages physical access devices. <role> issues authorization credentials for physical access to [COMPANY NAME] facilities and maintains a list of authorized personnel. Physical access devices include keys, locks, combinations, or card or badge readers.
2. Only [COMPANY NAME] personnel are authorized to deliver or remove IS components from the datacenter. The <role> controls key access to datacenter cabinets that contain components of the IS. Additions/removals of IS components are controlled/authorized and monitored by the <Change Control Board (CCB)>.
3. Physical access devices are managed using a [manual/automatic] process such as list of who is assigned access devices or updating the badge system as personnel change roles. The serial number of access devices are recorded and inspected on a quarterly basis. The badging system records the user’s name, location, email address, and office number. The badging system is audited quarterly and when personnel changes occur. Key card access is revoked, locks changed as needed, and badges are revoked when personnel leave or change jobs.

**PE.L2-3.10.2 – Protect and monitor the physical facility and support infrastructure for organizational systems:**

1. The physical facility where organizational systems reside is protected by the <FSO>, designee of, who monitors physical access within the [COMPANY NAME] facility to detect and respond to physical security incidents, including the use of video surveillance of all exterior doors. [COMPANY NAME] also employs and maintains fire suppression and detection devices/systems for the IS that are supported by an independent energy source In the event of a fire, fire detection devices/systems automatically activate to notify emergency responders and [COMPANY NAME] leadership. The physical facility where the CUI data is hosted is protected utilizing Microsoft Coverage for cloud-based services. However, remote employees are responsible for managing the physical security of their assigned workstations and respective work environment.
2. The support infrastructure for organizational systems where the CUI data is hosted is protected utilizing Microsoft Coverage for cloud-based services. [COMPANY NAME] also employs and maintains fire suppression and detection devices/systems for the on premises IS that are supported by an independent energy source In the event of a fire, fire detection devices/systems automatically activate to notify emergency responders and [COMPANY NAME] leadership.
3. The <FSO>, or designee of, monitors physical access within the [COMPANY NAME] facility to detect and respond to physical security incidents, including the use of video surveillance of all exterior doors. To accomplish this, personnel responsible for monitoring physical access:
   * Review physical access logs every 90 days.
   * Review physical access logs and video recordings upon the indication or realization of physical security incidents. This includes:
     + 1. Abnormal access times.
       2. Abnormal access patterns.
   * Coordinate the results of reviews and investigations with the organizational incident response capability, when determined necessary.
4. The support infrastructure for organizational systems where the CUI data is hosted is monitored utilizing Microsoft Coverage for cloud-based services. However, the support infrastructure for organizational systems is monitored utilizing the security guards and cameras around the perimeter of the building. Cameras also face the guard house and record vehicle licenses plates as they access the facility.

**PE.L2-3.10.6** – **Enforce safeguarding measures for CUI at alternate work sites. [COMPANY NAME] may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.**

1. Alternate work sites include the authorized alternate work site or the private residences of employees.
2. Due to the identified low integrity and availability levels, the consequences resulting from the loss of integrity and/or availability can be tolerated and overcome without significant impact to mission effectiveness or operational readiness. Contractual and mission operational requirements do not dictate that alternate site locations or redundant systems be deployed to provide uninterrupted service in the event of a failure or disaster. In the event of a prolonged outage, the following requirements shall apply:
   1. Alternate work sites may include government facilities or the private residences of employees.
   2. Only company provided laptops, tablets or desktops will be permitted to ensure that the same level of protection is afforded, including security controls, patch management, anti-virus protection and full disk (FIPS 140-2) encryption.
   3. Remote access to the internal enterprise network will only be permitted through the secure company VPN connection that disconnects the laptop/desktop from the remote network (i.e., prevents split tunneling).
   4. Access connections to the computer system and internal enterprise network require the use of multi-factor authentication: Microsoft Authenticator.
   5. Alternate site employees are to communicate with <FSO> in case of any security incidents and/or other security-relevant issues.

# Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Contact Information** |
|  |  |  |
|  |  |  |

# Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at [COMPANY NAME]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [COMPANY NAME] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
| V.01 | 11/282022 | Securestrux | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |