IS-10 FACILITY ACCESS POLICY

**10.1. Facility Access Policy**

<COMPANY NAME> works with Subcontractors to assure restriction of physical access to systems used as part of the <COMPANY NAME> Platform. <COMPANY NAME> and its Subcontractors control access to the physical buildings/facilities that house these systems/applications, or in which <COMPANY NAME> workforce members operate, in accordance to the HIPAA Security Rule 164.310 and its implementation specifications. Physical Access to all of <COMPANY NAME> facilities is limited to only those authorized in this policy. In an effort to safeguard ePHI from unauthorized access, tampering, and theft, access is allowed to areas only to those persons authorized to be in them and with escorts for unauthorized persons. All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to <COMPANY NAME>'s facility.

Of note, <COMPANY NAME> does not physically house any systems used by its Platform in <COMPANY NAME> facilities. Physical security of our Platform servers is outlined] (#1.4-<COMPANY NAME>-organizational-concepts).

**10.2 <COMPANY NAME>-controlled Facility Access Policies**

1. Visitor and third party support access is recorded and supervised. All visitors are escorted.
2. Repairs are documented and the documentation is retained.
3. Fire extinguishers and detectors are installed according to applicable laws and regulations.
4. Maintenance is controlled and conducted by authorized personnel in accordance with supplier-recommended intervals, insurance policies and the organization's maintenance program.
5. Electronic and physical media containing covered information is securely destroyed (or the information securely removed) prior to disposal.
6. The organization securely disposes media with sensitive information.
7. Physical access is restricted using smart locks that track all access.
	1. Restricted areas and facilities are locked when unattended (where feasible).
	2. Only authorized workforce members receive access to restricted areas (as determined by the Security Officer).
	3. Access and keys are revoked upon termination of workforce members.
	4. Workforce members must report a lost and/or stolen key(s) to the Security Officer.
	5. The Security Officer facilitates the changing of the lock(s) within 7 days of a key being reported lost/stolen.
	6. Networking equipment located within office facilities are secured against unauthorized physical access or tampering.
8. Enforcement of Facility Access Policies
	1. Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director, or the Privacy Officer.
	2. Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
	3. Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from <COMPANY NAME>.
9. Workstation Security
	1. Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities.
	2. All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
	3. All workstations purchased by <COMPANY NAME> are the property of <COMPANY NAME> and are distributed to users by the company.

**Purpose**

This policy is to ensure that the confidentiality, integrity, and availability of all <COMPANY NAME> data and information systems are protected by having in place appropriate controls for facility access, environmental protection (e.g. temperature/humidity control, fire detection/suppression), and alternate work sites.

**Scope**

This policy applies to all <COMPANY NAME> locations including any alternate processing centers used for disaster recovery. Additionally, all users of Company information systems are responsible for complying with and understanding this policy. This includes (but is not limited to) employees, consultants, contractors, vendors, business partners and temporary staff.

**Applicable Standards**

Applicable Standards from the HITRUST Common Security Framework

* 08.b - Physical Entry Controls
* 08.d - Protecting Against External and Environmental Threats
* 08.j - Equipment Maintenance
* 08.l - Secure Disposal or Re-Use of Equipment
* 09.p - Disposal of Media

Applicable Standards from the HIPAA Security Rule

* 164.310(a)(2)(ii) Facility Security Plan
* 164.310(a)(2)(iii) Access Control & Validation Procedures
* 164.310(b-c) Workstation Use & Security

# **Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description of changes** |
|  |  | **Initial creation** |
|  |  |  |
|  |  |  |