[Insert Company Name and Logo]	
Title: Information Technology Identity and Physical Access Control	**P&P #:**
Approval Date:	**Review: Annual**
Effective Date:	**Security Team**

Purpose: This Policy outlines procedures that limit physical access to any systems housing sensitive and regulated data and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed.

Scope: This policy applies to all employees and other members of the workforce (whether paid, contractor or volunteer) working in all facilities under the organization's ownership.

Policy: [Insert Company Name] maintains a Facility Access and Security Plan that outlines and documents its procedures to safeguard all facilities, systems, and equipment used to store sensitive and regulated data against unauthorized physical access, tampering, or theft. The Facility Access and Security Plan includes the following components:

Procedure:

Employee/Business Associate Access Controls and Validation

1. [Insert Company Name] implements appropriate procedures to control and validate employee access to all facilities used to house data systems.
2. [Insert Company Name] has adopted appropriate access control mechanisms to control physical access to all facilities containing sensitive and regulated data systems. [Code locks, badge readers, and key locks are examples of physical access control mechanisms.]
    a. Restricted areas and facilities are locked and alarmed when unattended (where feasible). Allowed access includes:
        i. Employees as approved by their supervisor as needed to perform their job duties.
        ii. Vendors (wearing Visitor ID badge) with an employee's escort into and out of the areas.
        iii. Vendors or Business Associates on a long-term contract (wearing a Visitor ID badge), once acclimated to the areas, without an escort.
    b. Only authorized employees and business associates receive keys/devices to access restricted areas (as determined by the Security Officer through Departmental requests).
    c. Employees are required to return keys/access devices to the Supervisor on their last day of employment/last day of contracted work or services being provided.
    d. Employees must report a lost and/or stolen key to the Security Officer. The Security Officer will facilitate the changing of the lock(s) within 24 hours of a key being reported lost/stolen, or disable the ID badge.
3. [Insert Company Name] implements appropriate procedures to identify all employees and business associates.
    a. All persons, are required to wear [Insert Company Name] identification badges. Employees will wear their ID badge at all times while at [Insert Company Name].
    b. Employees are required to return their [Insert Company Name] ID badge to the Human Resources department (or Supervisor) on their last day of employment/last day of contracted work or services being provided.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

c. Visiting vendors must register (sign in and out) on the Vendor Sign-in Log and obtain Visitor ID badges from the department they are visiting. Vendors are instructed to return the Visitor ID badge and sign out prior to leaving the premises.

4. [Insert Company Name] will adopt appropriate procedures to enforce this Policy. Violators out of restricted areas immediately and either have them register and obtain a visitor ID badge or escort them to the area they are trying to get to.
    a. Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director, or the Security Officer.
    b. Employees in violation of this policy are subject to disciplinary action, up to and including termination.
    c. Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services.
5. [Insert Company Name] has instituted appropriate procedures to maintain workstation security.
    a. Workstations may only be accessed and utilized by authorized employees or Business Associates wearing appropriate identification to complete assigned job/contract responsibilities. Third parties may be authorized by the Security Officer to access systems/applications on an as needed basis.
    b. All employees are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
    c. All [Insert Company Name] computer mainframes, servers, and network hardware are maintained in secured, locked, environmentally-conditioned rooms with 24 hour per day monitoring devices, which alert the Security Officer of any problems. Access to these rooms is limited to authorized IT and facility services employees as required to perform job responsibilities to maintain these rooms and/or the equipment within these rooms. Access by anyone else is granted only by approval from the Security Officer and only with an escort by an authorized IT or facility services workforce member.
    d. Permanent Workstations (i.e. desktop computer, printers, and monitors) may only be moved by authorized IT workforce members.
    e. All wiring associated with a workstation may only be installed, fixed, upgraded, or changed by an authorized IT workforce member or other individual authorized by the Security Officer.

Physical Access Records

1. List areas of your office/building that require physical access records. (Examples of areas requiring physical access records are computer, telephone and system rooms).
2. In addition to badge access, requires a signature log is required of all employees accessing [Insert Specified Area(s)].
3. Signature logs shall be maintained for six years (for heath records, other laws and statues may govern) from the date of creation, or the date it was last in effect, whichever is later [§164.530(j)].

Maintenance Records

1. Prior to approving plans to repair, modify, or scheduling maintenance, determine whether or not the scheduled maintenance, repairs, changes, or the construction process itself, increases the security risk to sensitive and regulated data. These security risks include, but are not limited to, work completed on the internal and/or external perimeter of the facilities (entryways, doors, locks, controlled access systems, walls, removing windows, etc.) and may result in:
    a. Will or has the potential to limit or remove an authorized user's ability to access workstations and systems in which sensitive and regulated data is created, received, maintained, or transmitted during regularly scheduled hours and at regularly scheduled locations.
    b. Increases the potential for unauthorized access to sensitive and regulated data.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

c. Otherwise has the potential to decrease the security, confidentiality, and/or integrity of the sensitive and regulated data in any way.

2. If the maintenance indicates an increased security risk to sensitive and regulated data, amend the plans to contain the following conditions:
    a. All users that need access to sensitive and regulated data have access during their regularly scheduled hours.
        i. If user will not have access to sensitive and regulated data, or complete systems during their regularly scheduled hours, the user or user's supervisor will be notified prior to the unavailability of the data and/or systems.
        ii. Document all decisions made and followed as required in this policy.
    b. If the plans increase the potential for unauthorized access to sensitive and regulated data, identify ways to secure said data throughout the project from unauthorized access.
        i. Implement 24-hour monitoring of the area with security guards or cameras.
        ii. Consider changing locks and distributing keys to individuals on the project to limit the number of individuals with access
        iii. Create new entryways for employees and/or patients.
        iv. Document all decisions made and followed as required in this policy.
        v. Continuously monitor the project and immediately notify affected employees of any increase or change in security risks to sensitive and regulated data and/or systems noted during the course of the project.
        vi. Document all decisions made and followed as required in this policy.
        vii. If a violation of facility access and security control policies and procedures is identified, it must be reported and investigated according to [Insert Company Name] Security Incident Policy.
    c. Document all meetings and other efforts made to protect the confidentiality, integrity, and availability of sensitive and regulated data and/or systems throughout the project, to include:
        i. Description of the repair or modification including a summary of the original plans, any changes made to the plans, and reasons for any changes made to the plans.
        ii. Reason for the repair or modification.
        iii. Repair or modification start and end dates.
        iv. Individual(s) that completed the repair or modification.
        v. Summary of all steps taken to eliminate or decrease the identified security risk(s) to include:
            1. Description of the identified security risk.
            2. Date the security risk was identified.
            3. Specify what was done to eliminate or reduce the security risk(s).
            4. Dates and times steps were taken to eliminate or reduce the security risk(s).
            5. Individuals involved in eliminating or reducing the security risk(s).
        i. After completion of the project, forward all documentation to the Security Officer.
        ii. The Security Officer maintains all documentation for a minimum of six years [§164.530(j)].

Violations: Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.

Attachments: None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

Related Policies:

- **Remote Access Policy**
- **Security Incident Policy**
- **Technical Safeguards, Access Control**

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.