Physical Access Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Technical support staff, system administrators, and security personnel are responsible for facility access requirements. The granting, controlling, and monitoring of physical access facilities is extremely important to an overall security program.

# II. Purpose

The purpose of this policy is to establish the rules for the granting, control, monitoring, and removal of physical access to ABC Company facilities.

# III. Scope

This policy applies to all Staff that use ABC Company Information Resources.

# IV. Policy

Physical access to all restricted facilities must be documented and managed. All facilities must be physically protected in proportion to the criticality or importance of their function.

Requests for access must come from the applicable data/system owner. Access to facilities must be granted only to support personnel, and contractors, whose job responsibilities require access to that facility. The process for granting card and/or key access to facilities must include the approval of the person responsible for the facility. The person responsible for the facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access. Access rights to facilities shall be based on the individual’s (i.e. Staff, visitor, contractor, etc.) role or function including control of access to software programs for testing and revision.

The Chief Security Officer (CSO) shall ensure:

* Secure areas are protected by appropriate entry controls that ensure only authorized personnel are allowed access.
* Procedures control and validate a staff member’s access to facilities with the use of guards, ID badges, key cards, etc.
* Procedures identify visitor controls such as visitor sign-in, wearing of visitor badges, escorting by authorized personnel, etc.
* Procedures for working in secure areas are designed and applied.
* Policies specify management’s review of the list of individuals with physical access to facilities containing sensitive information.
* A complete inventory of critical assets shall be maintained with ownership defined and documented.
* Card access records and visitor logs for facilities are kept for routine review based upon the criticality of the information being protected.

Access cards and/or keys must not be shared or loaned to others. Cards/keys must not be loaned or given to another individual. Cards/keys must not have identifying information other than a return mail address. Cards/keys that are no longer required must be returned to the person responsible for the facility. Lost or stolen cards/or keys must be reported to the person responsible for the facility. A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned. The person responsible for the facility must remove the card and/or key access rights of individuals that change roles or are separated from their relationship with ABC Company.

The person responsible for the facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

Procedures shall be developed to identify and authorize visitors:

* All facilities that allow access to visitors will track visitor access with a sign in/out log.
* A visitor log shall be used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where sensitive information is stored or transmitted. The visitor log shall document the visitor’s name, the firm represented, and the on-site personnel authorizing physical access on the log. The visitor log shall be retained for a minimum of three months, unless otherwise restricted by law.
* Visitors shall be identified and given a badge or other identification that expires and that visibly distinguishes the visitors from on-site personnel. Visitors shall surrender the badge or identification before leaving the facility or at the date of expiration.
* Visitors shall be authorized before entering, and escorted at all times within, areas where sensitive information is processed or maintained. Visitors must be escorted in card access-controlled areas of facilities.

Procedures shall be developed to easily distinguish between on-site personnel and visitors. Such controls to include, but not be limited to:

* Identifying new on-site personnel or visitors (e.g. assigning badges).
* Changes to access requirements.
* Revoking or terminating on-site personnel and expired visitor identification (e.g. ID badges).

Access to areas containing sensitive information must be physically restricted. All individuals in these areas must wear an identification badge on their outer garments so that both the picture and information on the badge are clearly visible.

Access to restricted IT areas such as data centers, computer rooms, telephone closets, network router and hub rooms, voicemail system rooms, and similar areas containing IT resources shall be restricted based upon business need.

Physical access to records containing confidential or protected data, and storage of such records and data in locked facilities, storage areas or containers shall be restricted.

Sensitive IT resources located in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access to sensitive information.

Appropriate facility entry controls shall limit and monitor physical access to Information Systems. Video cameras and/or access control mechanisms shall monitor individual physical access to sensitive areas. This excludes public-facing areas where only point-of sale terminals are present, such as cashier areas. Such data shall be stored for at least three months, unless otherwise restricted by law.

IT security Staff shall:

* Implement physical and/or logical controls to restrict access to publicly accessible data jacks. For example, data jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks. Areas accessible to visitors should not have data jacks enabled unless network access is specifically authorized.
* Restrict physical access to wireless access points, gateways, handheld devices, networking, communications hardware, and telecommunications lines.
* Control physical and logical access to diagnostic and configuration ports.
* Receive authorization prior to relocation or transfer of hardware, software or data to an offsite premise.

Physical access for on-site personnel to sensitive areas shall be controlled:

* Access must be authorized and based on individual job function.
* Access shall be revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., shall be returned or disabled.

Policies and procedures shall be established to ensure the secure use, asset management, and secure repurposing and disposal of equipment maintained and used outside the organization’s premises.

An appropriately cleared and technically knowledgeable Staff member shall be present within the area where maintenance is being performed to ensure that security procedures are followed.

* If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used, provided an appropriately cleared and technically qualified escort monitors and records the maintenance person's activities in a maintenance log. Uncleared maintenance personnel must be U.S. citizens.
* System initiation and termination shall be performed by the escort. In addition, keystroke monitoring shall be performed during access to the system.
* Prior to maintenance, the information system is completely cleared and all non-volatile data storage media shall be removed or physically disconnected and secured. When a system cannot be cleared, procedures identified in the System Security Plan shall be enforced to deny the maintenance personnel visual and electronic access to any Sensitive Information contained on the system.
* A separate, unclassified copy of the operating system, including any micro-coded floppy disks, CD-ROM, or cassettes that are integral to the operating system, shall be used for all maintenance operations. The copy shall be labeled “UNCLASSIFIED -- FOR MAINTENANCE ONLY” and protected in accordance with procedures established in the System Security Plan.

Processing of Sensitive Information shall only occur in approved areas. In addition:

* Devices that display or output information in human-readable form shall be positioned to prevent unauthorized individuals from reading the information.
* All personnel granted unescorted access to the area containing the Information System shall have an appropriate security clearance.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO10.05, APO11.09-10, APO12.02, APO13.07, DSS01.05, MEA01.05, MEA02.11

GDPR Article 25, 32

HIPAA 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(c) ,164.310(d)(1)

ISO 27001:2013 A.8.3.3, A.11.1

NIST SP 800-37 3.3, 3.6, 3.7

NIST SP 800-53 MP-5, PE-2-5, SC-42(3)

NIST Cybersecurity Framework PR.AC-1-2, PR.AC-4, PR.AC-6-7, PR.AT-1, PR.DS-5, PR.PT-1

PCI 8.6, 9.1-4, 9.9