Physical Security 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

Physical security is an essential part of an overall security plan. It forms the basis for all other security efforts, including data security.

# II. Purpose

Physical security ensures that ABC Company’s Information Resources are protected by physical security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

# III. Scope

This policy applies to all ABC Company Staff responsible for the security of ABC Company’s facilities and related resources.

# IV. Policy

Physical security refers to the protection of building sites and equipment (and all other information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g. electrical surges, extreme temperatures, spilled liquids). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders. Physical protection against natural disasters, malicious attack, or accidents shall be designed and applied.

Each Department is required to have a Facility Security Plan (Plan) which includes measures to safeguard Information Resources. The Plan shall describe ways in which all Information Resources are protected from physical tampering, damage, theft, or unauthorized physical access. Procedures shall be established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas.

Physical and environmental security controls protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. ABC Company's physical and environmental security program prevents interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft.

Physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) shall be implemented to safeguard sensitive data, information systems, and information processing facilities.

Physical controls and attestation mechanisms shall be designed to address legislative requirements. The results shall be shared with ABC Company management and cloud computing tenants.

Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing servers and data.

* Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
* Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
* Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage. Procedures shall monitor, control, and protect communications at external boundaries and at key internal boundaries of Information Systems.
* Equipment shall be correctly maintained to ensure its continued availability and integrity.
* Equipment, information, or software shall not be taken off-site without prior authorization.
* Security shall be applied to off-site assets taking into account the different risks of working outside the organization’s premises.
* All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
* Users shall ensure that unattended equipment has appropriate protection.
* When leaving their work area, users shall ensure that their desk and work area is clear (clear desk) of papers and removable storage media. In addition, monitors shall be cleared (clear screen) to protect against unauthorized access to information or information systems. See the Clear Desk Policy for more information.
* Physical access controls address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation.
* It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied.
* Each individual that is granted access rights to a facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.

All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes. Building fires are a particularly important security threat because of the potential for complete destruction of both hardware and data as well as the risk to human life. Smoke, corrosive gases and high humidity from a localized fire can damage systems throughout an entire building. Security personnel must evaluate the fire safety of buildings that house systems.

Systems and the people who operate them need to have a reasonably well-controlled operating environment. Failures of electric power, heating and air-conditioning systems, water, sewage, and other utilities will usually cause a service interruption and may damage hardware. ABC Company Staff must ensure that these utilities, including their many elements, function properly.

Staff must be made aware that a building may be subjected to a load greater than it can support. Commonly, this is a result of an earthquake, explosion that displaces or cuts structural members, or a fire that weakens structural members.

While plumbing and roof leaks do not occur every day, they can be seriously disruptive. Staff must know the location of plumbing lines that might endanger system hardware and take steps to reduce risk (e.g., moving hardware, relocating plumbing lines, and identifying shutoff valves).

IT equipment must be marked with some form of identification that clearly indicates it is the property of ABC Company. Refer to the Data Marking Policy for additional information in this area.

The Chief Security Officer shall ensure:

* Policies and procedures safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
* Policies and procedures include controls such as locked doors, signs warning of restricted areas, surveillance cameras, alarms, property controls (property asset tag, engravings), and personnel controls (ID badges, visitor badges, escorts), security service or patrol of the facility.
* Policies and procedures specify how to document facility repairs and modifications.
* Policies and procedures specify all physical security components that require documentation.
* Policies and procedures identify special circumstances when repairs or modifications to physical security components are required such as when special staff members with special access (e.g. application administrators) are terminated.
* Procedures document the process to test data center environmental controls (e.g. electrical power, battery backups, and air conditioning) on a quarterly basis. Such activities shall be recorded in a log.
* Workstation physical safeguards restrict access only to authorized users.
* Procedures specify physical safeguards for workstations and other devices that access, receive, transmit, process, or store sensitive information.
* Procedures identify devices (e.g. workstations, desktops, laptops, tablets, smartphones, etc.) that are allowed to access systems containing sensitive information.
* Physical safeguards are effective at protecting workstations and other devices that access, receive, transmit, process, or store sensitive information.
* Procedures identify when additional physical safeguards are needed to protect workstations and other devices that access, receive, transmit, process, or store sensitive information.
* Access points such as delivery, loading, and other points where unauthorized persons could enter the premises are controlled, and, if possible, isolated from information processing facilities to avoid unauthorized access.

# 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 Department Heads and those responsible for information and physical security.

**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