

Physical Security and Environmental Protection Policy

Purpose

Information security depends on physical security — a server that can be walked out the door or a workstation left unlocked in a public area undermines every logical control layered on top of it. This policy defines how Your Organization controls physical access to its facilities and equipment, and protects information systems from environmental hazards such as fire, power loss, and water damage.

Scope

This policy applies to all Your Organization-controlled facilities that house information systems or store Confidential or Restricted data — offices, data centers, and any leased or shared space under Your Organization's operational control. Where Your Organization relies on third-party data centers or colocation facilities, this policy is satisfied through vendor due diligence per the Vendor Risk Management Policy rather than direct control.

Physical access authorization

- Physical access to Your Organization facilities, and to restricted areas within them (server rooms, network closets, secure storage), is granted only to individuals with a documented business need and is approved by the facility or system owner.
- Access credentials (badges, keys, key cards) are individually assigned — not shared — and tied to an identity in the access control system.
- Access to restricted areas is reviewed at least quarterly, consistent with the Access Control Policy's review cadence for privileged access.

Visitors and contractors

- Visitors, including contractors without standing access, must sign in, be issued a visible visitor credential, and be escorted by an authorized workforce member while in non-public areas.
- Visitor entries and exits are logged, including the sponsoring employee.

Monitoring and access logging

- Facilities housing information systems are monitored via badge-access logging and, where applicable, video surveillance and intrusion alarms.
- Physical access logs and video retention are kept for a period consistent with the Data Retention Policy, and are reviewed periodically or upon a suspected physical security incident.

Equipment and workspace security

- Workstations and portable devices must be locked or secured when unattended, and screens locked after a defined period of inactivity (see the Password and Authentication Policy).
- Sensitive documents and portable media are not left unattended in view in shared or public workspaces ("clean desk" expectation for Confidential and Restricted material).
- Server and network equipment is housed in locked racks or rooms with access limited to authorized IT and Facilities personnel.

Environmental protections

- Facilities housing production information systems maintain appropriate fire detection and suppression, temperature and humidity control, and uninterruptible power supply or generator backup proportional to the criticality of the systems housed.
- Environmental controls are tested and maintained on a schedule set by Facilities, with results retained as evidence of operability.

Alternative work sites

Remote and hybrid workforce members are expected to take reasonable precautions to protect company equipment and data at home or other alternative work sites — including physical security of devices, avoiding shoulder-surfing risk in public spaces, and prompt reporting of lost or stolen equipment. See the Acceptable Use Policy for endpoint-specific expectations.

Incident reporting

Suspected physical security incidents — tailgating, lost badges, unattended access points, unauthorized individuals in restricted areas — must be reported immediately to Facilities and Information Security and, where they may involve data exposure, handled per the Incident Response Plan.

Roles and responsibilities

- **Facilities.** Owns physical access control systems, visitor management, and environmental controls.
- **IT Operations.** Owns physical security of server rooms and network equipment.
- **Information Security.** Reviews physical access logs and incorporates physical risk into the overall risk assessment program.

Review cadence

This policy is reviewed annually by Facilities and Information Security, or sooner following a physical security incident or a change of facility.

Effective date: [the date this policy takes effect]