Physical Security Policy

Doorway

SOC 2 Criteria: CC6.4
ISO 27001 Annex A: A.11.1, A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.5, 11.2.6

Keywords: Facilities, Office visitors, Access Requirements, Asset Security

---

Purpose

The Physical Security Policy establishes requirements to ensure that Doorway's information assets are protected by physical controls that prevent tampering, damage, theft or unauthorised physical access. This policy defines the following controls and acceptable practices:

- Definition of physical security perimeters and required controls
- Personnel and visitor access controls
- Protection of equipment stored off-site

Scope

This policy applies to all Doorway physical facilities and users of information systems within Doorway, which typically include employees and contractors, as well as any external parties that have physical access to the company's information systems. This policy must be made readily available to all users.

Background

It is the goal of Doorway to safeguard information both virtually and physically, as well to provide a safe and secure environment for all employees. As such, access to the Doorway facilities is limited to authorised individuals only. All workforce members are responsible for reporting an incident of unauthorised visitor and/or unauthorised access to Doorway's facility.

Roles and Responsibilities

The Security Officer is responsible for updating, reviewing, and maintaining this policy.

Policy

General

- Physical access to Doorway facilities is restricted.
- All employees are required to wear employee badges at secure facilities if and when applicable (such as server rooms, data centres, labs).
- All employees must follow physical security requirements and procedures documented by facility management.
- On-site visitors and vendors must be escorted by a Doorway employee at all times while on premise.
- All workforce members are responsible for reporting an incident of unauthorised visitor and/or unauthorised access to Doorway's facility.
- A record is retained for each physical access, including visits, maintenance and repairs to Doorway production environments and secure facilities.
    - Details must be captured for all maintenance and repairs performed to physical security equipment such as locks, walls, doors, surveillance cameras; and
    - All records must be retained for a minimum of seven years.
- Building security, such as fire extinguishers and detectors, escape routes, floor warden responsibilities, shall be maintained according to applicable laws and regulations.

Access Requirements

- Physical access is restricted using badge readers and/or smart locks that track all access.
    - Restricted areas and facilities are locked when unattended (where feasible).
    - Only authorised workforce members receive access to restricted areas (as determined by the Security Officer).
    - Access and keys are revoked upon termination of workforce members.
    - Workforce members must report a lost and/or stolen key(s) or badge(s) to his/her manager, local Site Lead, or the Facility Manager.
    - The Facility Manager or designee is responsible to revoke access to the lost/stolen badge(s) or access key(s), and re-provision access as needed.
    - The Facility Manager or designee facilitates the changing of the lock(s) within 7 days of a physical key being reported lost/stolen.
- Visitor access requires additional controls.

  - Visitors must sign a visitor's log indicating date and time in/out, organisation represented (if applicable), purpose of visit, and company point of contact.
  - Visitor badges will be issued to visitors, and must be displayed at all times when in secure areas. Badges must be returned before leaving the facility or by the specified time.
- Delivery and Loading areas.
  - Access to delivery and loading areas from outside of the facility will be restricted to only identified and authorised personnel.
  - Such areas will be designed to ensure that access to other parts of the facility are restricted.
  - Incoming material must be appropriately inspected for any discrepancies, issues, or potential threats, and must be registered in accordance with *Asset Management* procedures.
  - When possible, incoming and outgoing shipments will be physically segregated.
- Enforcement of Facility Access Policies
  - Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director, or the Privacy Officer.
  - Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
  - Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from Doorway.
- Workstation Security
  - Workstations may only be accessed and utilised by authorised workforce members to complete assigned job/contract responsibilities.
  - All workforce members are required to monitor workstations and report unauthorised users and/or unauthorised attempts to access systems/applications as per the System Access Control Policy.
  - All workstations purchased by Doorway are the property of Doorway and are distributed to personnel by the company.

Building Standards per Location

Standards

- A security perimeter must be defined and established to protect areas containing sensitive data and critical information processing facilities.
- The walls, ceilings and floor of any secure area must be of the same strength.
- Windows and doors have locks, and all entry points are secured by access control mechanisms and have cameras for additional monitoring as needed.
- Spaces around the perimeter are monitored with CCTV or security patrols.
  - CCTV recordings need to be kept for at least 3 months.
- Alarms are activated outside working hours.
- The most sensitive assets must be stored in the most secure areas. Using the "onion technique", each perimeter "layer" should house progressively more sensitive assets.

- Keys to all secure or public areas housing IT equipment (including wireless access points, gateways, and more) must be protected in a centralised fashion.
- A controlled reception area must establish where:
    - All visitors are required to report first.
    - Security guards challenge unknown persons.
- Offsite backup locations are physically secure for backups and the security measures are reviewed at least annually.

Location(s)

- London Office:
    - The building is unlocked Monday-Friday from 9am-4pm
    - After hours the building is secured and requires an access card for entry
    - The office is secured and requires an access card for entry for after hours access
    - All server rooms are secured 24/7 and require an access card for entry

Data Center Security

Physical security of data centres is ensured by Doorway's cloud infrastructure service provider.

Asset Security

The following factors will be considered and implemented, as applicable per risk assessments, and in conjunction with the following policies: *Information Security Policy*, *Asset Management Policy*, *Data Protection* and *Data Classification*:

External/Environmental Threats

All assets owned or managed by Doorway will be housed in designated facilities with a level of protection equivalent to the sensitivity and criticality of the asset and the associated information. Additionally, the following factors will be considered:

- The potential danger from environmental threats including weather, malicious attacks, and accidents.
    - Appropriate for risk mitigation must be implemented to reduce the potential for an incident to occur.
- Monitoring environmental conditions in appropriate areas.
    - At a minimum, monitoring will be performed for fire/smoke in the general facility areas.
    - Internal secure areas must be subject to additional monitoring for temperature, water, power continuity, humidity and cleanliness.
- Implementation of environmental controls in accordance with risk assessments.

    - Controls such as heating, ventilation, air conditioning, drainage, fire suppression, emergency lighting, continuous power and humidity control must be implemented in facilities, as appropriate.
    - If applicable, data centres must contain elements of each environmental control at sufficient levels.

Backup Power

Continuous power will be provided for mission-critical information assets through battery-operated uninterrupted power supply (UPS) protection.

- Backup generators will be used in cases of higher levels of protection.

Emergency Power Shutoff

In the case of emergency, emergency power-off switches will be located near emergency exits in equipment rooms to facilitate rapid power down.

Alarm systems

Alarm system configurations must be periodically reviewed and evaluated to detect malfunctions in the supporting utilities and reconfigured when necessary.

Off-Site Equipment and Security

Equipment may only be taken off-site for valid business reasons and with authorisation from the Information Security Owner.

- The equipment includes network and telecommunication devices, servers, power and cooling equipment
- Individuals taking equipment offsite are responsible for the physical protection of the system and must ensure the system is secured at all times.
- Equipment will be recorded as being removed off-site and recorded when returned.

Cabling Protection

Power and telecommunications cabling must be protected adequately against risks such as interference, data capture or physical damage.

- Cables must be easily identifiable through markers or labels to ensure minimal handling errors.

Revision History

Version	Date	Editor	Description of Changes
1.0	15.03.2022	Henry Sinclair	Initial Creation