Physical Security Policy Template, version 1.0.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document Owner: Olumuyiwa Agunbiade
Last Review Date: November 2023

Physical Security Policy Template

Purpose

The purpose of the Physical Security Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to (Company Name) Information Resource facilities.

Audience

The Physical Security Policy applies to all individuals that install,support, maintain, or are otherwise responsible for the physical security of (Company) **Information Resources**.

Contents

Policy

General

- Physical security systems must comply with all applicable regulations including but not limited to building codes and fire prevention codes.
- Physical access to all (Company) restricted facilities must be documented and managed.
- All **Information Resource** facilities must be physically protected in proportion to the criticality or importance of their function at (Company).
- Access to **Information Resources** facilities must be granted only to (Company) support personnel and contractors whose job responsibilities require access to that facility.
- All facility entrances, where unauthorized persons could enter the premises, must be controlled.
- Secure areas must be protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. This includes:
    - information processing facilities handling **confidential information** should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use;
    - **controls** should be adopted to minimize the risk of potential physical and environmental threats;

    - environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities.
- Equipment must be protected from power failures and other disruptions caused by failures in utilities.
- Restricted access rooms and locations must have no signage or evidence of the importance of the location.
- All **Information Resources** facilities that allow access to visitors will track visitor access with a sign in/out log.
- Card access records and visitor logs for **Information Resource** facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- Visitors in controlled areas of **Information Resource** facilities must be accompanied by authorized personnel at all times.
- Personnel responsible for **Information Resource** physical facility management must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

Access Cards

- The process for granting card and/or key access to Information Resource facilities must include the approval of physical security personnel.
- Each individual that is granted access to an **Information Resource** facility must sign the appropriate access and non-disclosure agreements.
- Cards must not be reallocated to another individual, bypassing the return process.
- Physical security personnelmust remove the card and/or key access rights of individuals that change roles within (Company) or are separated from their relationship with (Company).
- Physical security personnel 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.

Utility Systems

- All utility systems in use at the facility must be identified and documented with detailed procedures for overall maintenance requirements.
- Maintenance and testing activities must be performed in accordance to manufacturers specifications and must be documented to provide an audit trail of all activities.
- Utility systems must be secured from unauthorized access.
- Utility systems must be set to alarm on malfunctions.
- Emergency systems, lighting, fire suppression, and emergency power systems, must be in place and tested regularly to ensure functionality.
- Critical utilities must be configured in a redundant manner to ensure continued functionality.

Housekeeping (if thirdparty)

- Housekeeping/cleaning staff must go through standard **information security awareness** training.
- Where external or third parties are used for cleaning services, the third party must be insured and bonded.
- Housekeeping/cleaning staff must have adequate and approved background checks performed.

- Housekeeping/cleaning staff must be (supervised/monitored)while performing required duties.
- Housekeeping/cleaning staff must wear uniforms, badges, and be assignedaunique identifier that provides an audit trail on access to areas of the facility.
- If housekeeping/cleaning staff need to gain access to restricted areas specific clearance from security staff must be obtained.

Loading Docks

- Proceduresfor delivery and receipt of packages must be documented.
- Delivery areas must be secured and isolated from public areas.
- External doors of the delivery area must be secured when internal doors are open.
- Delivery areas must belocked when unattended. Unauthorized personnel must be accompanied at all times within delivery areas.
- Surveillance cameras must be secured and adequately cover delivery areas.
- Incoming deliveries must be registered, isolated, and inspected for evidence of tampering before being moved to internal areas.
- All discovered evidence of tamperingmust immediately be reported to physical security personnel.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 7, 9, 11, 13, 16
- NIST CSF: PR.AC, PR.IP, PR.PT, DE.CM
- Continuity and Recovery Policy
- Incident Management Policy

Waivers

Waivers from certain policy provisions may be sought following the (Company) Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	November 2023		Olumuyiwa Agunbiade	Document Origination

Question & Answer?