[INSERT FIRM LEGAL NAME]

Physical Security Policy

[Insert Firm Logo]

Version 1.0

[Insert Date]

[Insert Firm Logo]

Contents

Instructions

Documents are in a template format and are to be customized to fit the appropriate business and operational requirements. Use the sample as a foundation to build a bespoke policy for your business.

If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company specific document. **Otherwise, it would be a liability exposure to establish a policy and not to comply with it.**

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of the policy subject. Businesses should deploy a defense-in-depth security model of technical, operational, and physical security controls.

Delete the instructions after finalizing and adopting the policy.

Policy Overview

The purpose of the <CompanyName> Physical Security Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities.

Scope and Purpose

The (District/Organization) Physical Security Policy applies to all <CompanyName> individuals that install and support Information Resources, are charged with Information Resource security and data owners.

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 <CompanyName> 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 <CompanyName>.
- Access to Information Resources facilities must be granted only to <CompanyName> support personnel and contractors whose job responsibilities require access to that facility.

- All facility entrances, where unauthorized persons could enter the premises, must be checked.
- 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.

- Directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.
- 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 a member of the physical security committee.
- Each individual that is granted access rights to an Information Resource facility must sign the appropriate access and non-disclosure agreements.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to personnel responsible for Information Resource physical facility management. Cards must not be reallocated to another individual, bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for Information Resource physical facility management physical security committee as soon as possible.
- Physical security committee must remove the card and/or key access rights of individuals that change roles within <CompanyName> or are separated from their relationship with <CompanyName>.
- Physical security committee 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.

Compliance

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.

Exceptions

Waivers from certain policy provisions may be sought following the <CompanyName> Waiver Process.

Definitions and Terms

None

Appendix

None

Revision Table

Revision History				
#	**Version #**	**Date**	**Updates/Changes**	**Owner**
1	1.0	2022	Initial Draft	Riskigy
2				