

{Insert Company Name}

Security Policy

Physical and Environmental Security

**Version:**

{N.N}

**Date:**

{Insert Modified Date}

# Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Any item that needs to be updated within this document can be found with { } around each item and in (RED) Font. [Delete this for final product submission]

# Table of Contents

1 Introduction ............................................................................................................................................. 1

2 Purpose .................................................................................................................................................... 1

3 Scope ........................................................................................................................................................ 2

4 Roles and Responsibilities ........................................................................................................................ 2

5 Management Commitment ..................................................................................................................... 2

6 Authority .................................................................................................................................................. 3

7 Compliance .............................................................................................................................................. 3

8 Policy Requirements ................................................................................................................................ 4

8.1 Physical and Environment Protection Policies and Procedures [PE-1] ............................................ 4

8.2 Physical Access Authorizations [PE-2] .............................................................................................. 4

8.3 Physical Access Control [PE-3, {PE-3 (1) High Only}] ........................................................................ 4

8.4 Access Control for Transmission [PE-4] ............................................................................................ 5

8.5 Access Control for Output Devices [PE-5] ........................................................................................ 5

8.6 Monitoring Physical Access [PE-6, PE-6 (1), {PE-6 (4) High Only}] ................................................... 5

8.7 Visitor Access Records [PE-8, {PE-8 (1) High Only}] .......................................................................... 6

8.8 Power Equipment and Cabling [PE-9] .............................................................................................. 6

8.9 Emergency Shutoff [PE-10] .............................................................................................................. 6

8.10 Emergency Power [PE-11, {PE-11 (1) High Only}] .......................................................................... 6

8.11 Emergency Lighting [PE-12] ........................................................................................................... 6

8.12 Fire Protection [PE-13, PE-13 (1,2)] ............................................................................................... 6

8.13 Environmental Controls [PE-14, {PE-14 (2) High Only}] ................................................................. 7

8.14 Water Damage Protection [PE-15, {PE-15 (1) High Only}] ............................................................. 7

8.15 Delivery and Removal [PE-16] ........................................................................................................ 7

8.16 Alternate Work Site [PE-17] ........................................................................................................... 7

8.17 Location of System Components [{PE-18 High Only}] ................................................................... 8

# Introduction

{Insert Company Name} has developed corporate policies that identify the security requirements for its information systems and personnel in order to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by {Insert Company Name}’s management and in compliance with the Access Control family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of {Insert Company Name}’s systems, facilities, and data are protected. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these policies pertain to all {Insert Company Name} employees, contractors, third parties, and others who have access to company and customer confidential information within {Insert Company Name} systems and facilities.

# Roles and Responsibilities

These policies apply to all {Insert Company Name} employees, contractors, business partners, third parties, and others who need or have access to {Insert Company Name}’s systems and our customer's confidential information. {Insert Company Personnel below and delete this for final product}

|  |  |  |
| --- | --- | --- |
| **Individual or Group** | **Role** | **Responsibility** |
|  | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. |
|  | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program. |
|  | Information Owner | Has statutory, management, or operational authority for {Insert Company Name} information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal. |
|  | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
| **Individual or Group** | **Role** | **Responsibility** |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Chief Information Security Officer | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Security Manager | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Technology Director | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
|  | Information System Security Officer | Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures. |
| System Admin Team | System Administrator | Responsible for conducting information system security Administration activities. |
| Varies | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures. |
| Varies | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

{Insert Company Name} and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the {Insert Company Name} Information System by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the {Insert Company Name} Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002
2. Federal Information Security Modernization Act of 2014 (FISMA)
3. The Privacy Act of 1974
4. Clinger-Cohen Act of 1996
5. OMB Circulars and Memoranda
6. Federal Information Processing Standards (FIPS)
7. NIST Special Publications
8. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
9. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011

# Compliance

Compliance with these policies is mandatory. It is {Insert Company Name}’s policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed by an external vendor and/or internal self-assessments to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team’s recommendations.

# Policy Requirements

The following personally identifiable information processing and transparency controls requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support information systems owned and operated by {Insert Company Name}, including its subsidiaries and affiliates, collectively referred to as {Insert Company/Product Name}.

The following access control requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the {Insert Company/Product Name} information systems.

8.1 Physical and Environmental Policies and Procedures [PE-1]

This document is intended to serve as the *Physical and Environmental Protection Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Physical and Environmental Protection Policy* and related controls have been developed, documented, and disseminated to all applicable personnel.

{Insert Company Name} must develop, document, and disseminate to all personnel including the chief privacy officer, ISSO, and/or similar roles or their designees: [PE-1 (a)]

* An organizational-level Physical and Environmental Protection Policy that: [PE-1 (a) (1)]
  + Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance [PE-1 (a) (1) (a)]
  + Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines [PE-1 (a) (1) (b)]
* Procedures to facilitate the implementation of Physical and Environmental Protection Policy and the associated Physical and Environmental Protection controls [PE-1 (a) (2)]

{Insert Company Name} must designate a Chief Information Security Officer (CISO) to manage the development, documentation, and dissemination of the Physical and Environmental Protection policy and procedures. [PE-1 (b)]

{Insert Company Name} must review and update the current Physical and Environmental Protection: [PE-1 (c)]

* Policies at least annually, following a significant change, and/or any compromising event [PE-1 (c) (1)]
* Procedures at least annually, following a significant change, and/or any compromising event [PE-1 (c) (2)]

8.2 Physical Access Authorizations [PE-2]

For the facilities hosting the information system, a list of personnel with authorized access to the facility (except for those areas within the facility officially designated as publicly accessible) has been developed and must be kept up to date. [PE-2 (a)] Only authorized personnel may be issued access credentials. [PE-2 (b)] The facility access list shall be reviewed and authorized at least annually or every 90 days (for high impact systems only) and personnel who no longer require access shall be removed from the authorized access list. [PE-2 (c)] Authorization credentials for facility access will be issued to those individuals with appropriate access clearance. [PE-2 (d)]

8.3 Physical Access Control [PE-3, {PE-3 (1) High Only}]

For the facilities hosting the information system, physical access authorizations must be enforced for all physical access points, including designated entry and exit points, at the facility. [PE-3 (a)] Physical security shall be enforced through verifying individual access authorizations before access is granted to the facility [PE-3 (a) (1)] and controlling entry to the facility using physical access control devices and/or guards. [PE-3 (a) (2)]

Access to areas officially designated as publicly accessible are controlled in accordance with {Insert Company Name}’s assessment of potential risk. [PE-3 (c)] For all other areas not considered publicly accessible, the following physical security measures will be observed:

* Physical access audit logs must be maintained for entry/exit points [PE-3 (b)]
* Visitors must be escorted to their destination and monitored [PE-3 (d)]
* Keys, combinations, and other physical access devices must be secured [PE-3 (e)]
* Physical access devices must be inventoried at least annually [PE-3 (f)]
* For areas secured with a combination and key lock, combinations and keys must be changed at least annually and/or when keys are lost, combinations are compromised, or when an employee is transferred or terminated [PE-3 (g)]

**For high impact systems only:**

* Enforce physical access authorizations to the system in addition to the physical access controls for the facility at any access point to areas containing components of a high impact system. [PE-3 (1)]

8.4 Access Control for Transmission [PE-4]

{Insert Company Name} must control physical access to system distribution and transmission lines within its facilities using physical and logical access restrictions. [PE-4]

8.5 Access Control for Output Devices [PE-5]

{Insert Company Name} must control physical access to output devices, such as monitors and printers, to prevent unauthorized individuals from obtaining the output. [PE-5]

8.6 Monitoring Physical Access [PE-6, PE-6 (1), {PE-6 (4) High Only}]

{Insert Company Name} must ensure that physical access to the facilities hosting information systems are controlled to allow security personnel to detect and respond to physical security incidents. The following security measures are mandatory to support this objective:

* Physical access to the facility where systems are hosted must be monitored to detect and respond to physical security incidents [PE-6 (a)]
* Physical access logs must be reviewed at least monthly and upon occurrence of any security event or potential indications of an event [PE-6 (b)]
* Results of reviews and investigations are coordinated with facility incident response capability [PE-6 (c)]
* Real-time physical intrusion alarms and surveillance equipment are monitored on a regular basis [PE-6 (1)]

**For high impact systems only:**

* Monitor physical access to the system in addition to the physical access monitoring of the facility at key restricted areas [PE-6 (4)]

8.7 Visitor Access Records [PE-8, {PE-8 (1) High Only}]

Information system hosting facilities visitor access records must include: [PE-8]

* + Names and organizations of persons visiting
  + Forms of identification
  + Dates of access
  + Entry times
  + Purpose of visit
  + Names and organizations of person(s) visited / Escort
* All visitor access records for the facility are reviewed at least monthly [PE-8 (b)] and maintained for a minimum of one (1) year [PE-8 (a)]
* Anomalies in visitor access records must be reported to facilities management [PE-8 (c)]

**For high impact systems only:**

* Maintain and review access records using the facility’s visitor log system [PE-8 (1)]

8.8 Power Equipment and Cabling [PE-9]

All power equipment and power cabling for the facilities hosting the Information System must be protected from damage and destruction. [PE-9]

8.9 Emergency Shutoff [PE-10]

For the facilities hosting the Information System, authorized individuals have access and the capability to shut off power to the system or individual system components in the event of an emergency. [PE-10 (a)] Emergency shutoff switches or devices must be placed in locations that facilitate safe and easy access to authorized personnel. [PE-10 (b)] Additionally, emergency power shutoff capability must be protected from unauthorized activation. [PE-10 (c)]

8.10 Emergency Power [PE-11, {PE-11 (1) High Only}]

{Insert Company Name} must ensure that a short-term uninterruptible power supply is provided to facilitate an orderly shutdown of system components or transition of the system to long-term alternate power in the event of a primary power source loss at facilities hosting its Information Systems. [PE-11]

**For high impact systems only:**

* Alternate power supply with minimal operating capability can be satisfied, automatically by accessing a secondary commercial power or other external power supply. [PE-11 (1)]

8.11 Emergency Lighting [PE-12]

{Insert Company Name} must ensure that automatic emergency lighting is employed and maintained at the facilities hosting information systems. The lighting should activate in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility. [PE-12]

8.12 Fire Protection [PE-13, PE-13 (1,2)]

{Insert Company Name} must ensure that the following fire protection measures have been put in place and must be maintained for the facilities hosting information systems:

* Fire suppression and detection devices/systems that are supported by an independent energy source are employed and maintained [PE-13]
* Fire detection devices/systems that activate automatically and notify building manager and emergency responders in the event of a fire are employed [PE-13 (1)]
* Fire suppression devices/systems that provide automatic notification of any activation to emergency responders are employed [PE-13 (2) (a)]
* An automatic fire suppression capability is employed when the facility is not staffed on a continuous basis [PE-13 (2) (b)]

8.13 Environmental Controls [PE-14, {PE-14 (2) High Only}]

{Insert Company Name} must ensure that the following temperature and humidity controls have been put in place and must be maintained for the facilities hosting the information system:

* Temperature and humidity levels are consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments and temperature at server inlets and humidity levels by dew point are measured [PE-14 (a)]
* Environmental control levels are continuously monitored [PE-14 (b)]

**For high impact systems only:**

* Audible and visual environmental notifications alert responsible and nearby personnel of changes to potentially harmful to personnel or equipment [PE-14 (2)]

8.14 Water Damage Protection [PE-15, {PE-15 (1) High Only}]

{Insert Company Name} must ensure that system components are protected from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel within facilities hosting information systems. [PE-15]

**For high impact systems only:**

{Insert Company Name} must ensure that facilities hosting the information system use water detection sensors tied to an automatic notification system to alert the facility manager and responsible personnel. [PE-15 (1)]

8.15 Delivery and Removal [PE-16]

{Insert Company Name} must ensure that all components entering and exiting the facilities hosting information systems facility must be authorized, monitored, and controlled and that records of those items are maintained. [PE-16]

8.16 Alternate Work site [PE-17]

{Insert Company Name} have determined and documented that all employees are permitted to utilize any alternate work location [PE-17 (a)] provided that the following conditions are satisfied: [PE-17 (b)]

* Unless otherwise approved, employees are only permitted to work at alternative work sites located in the United States. (See CM Policy Section 8.2.1)
* Personnel may not disable any security software or configurations established on their company issued device
* Personnel must connect company property to the corporate VPN at alternate work sites over an encrypted connection
* Personnel must take precautions to prevent shoulder surfing when working in public areas
* Personnel must secure their {Insert Company Name} equipment in a locked container, room, or building or otherwise tether their equipment when not in use by the employee to prevent theft

{Insert Company Name} must assess the effectiveness of security controls at alternate work sites on an ongoing basis [PE-17 (c)]

{Insert Company Name} must provide a means for personnel to communicate with Information Security personnel in case of security incidents or problems [PE-17 (d)]

8.17 Location of System Components [{PE-18 High Only}]

**For high impact systems only:**

{Insert Company Name} must ensure that system components are located within the hosting facility to minimize potential damage from physical and environmental hazards; to minimize the opportunity for unauthorized access; and to protect the system from any physical and environmental hazards identified during a threat assessment.