

{Insert CompanY Name}

Security Procedures

Physical & Environmental [PE]

**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 Procedural Requirements ........................................................................................................................ 4

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

8.2 Physical Access Control [PE-3] .......................................................................................................... 4

8.3 Access Control for Transmission Medium [PE-4] ............................................................................. 6

8.4 Access Control for Output Devices [PE-5] ........................................................................................ 6

8.5 Monitoring Physical Access [PE-6] ................................................................................................... 6

8.6 Visitor Access Records [PE-8] ........................................................................................................... 6

8.7 Power Equipment and Power Cabling [PE-9] ................................................................................... 7

8.8 Emergency Shutoff [PE-10] .............................................................................................................. 7

8.9 Emergency Power [PE-11] ................................................................................................................ 7

8.10 Emergency Lighting [PE-12] ........................................................................................................... 8

8.11 Fire Protection [PE-13] ................................................................................................................... 5

8.12 Temperature and Humidity Controls [PE-14] ................................................................................. 5

8.13 Water Damage Protection [PE-15] ................................................................................................. 5

8.14 Delivery and Removal [PE-16] ........................................................................................................ 5

8.15 Alternate Work Site [PE-17] ........................................................................................................... 5

# 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}’ 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}’ 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}’ 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}’ 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.

# Procedural Requirements [PE-1]

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

## Physical Access Authorizations [PE-2]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

Or

{Insert Company Name} shall ensure the following:

1. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides
2. Issue authorization credentials for facility access
3. Review the access list detailing authorized facility access by individuals at least annually
4. Remove individuals from the facility access list when access is no longer required

## Physical Access Control [PE-3]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} shall do the following:

* 1. Enforce physical access authorizations at any entry and exit points to the facility where the system resides by:
     1. Verifying individual access authorizations before granting access to the facility
     2. Controlling ingress and egress to the facility using {Listed Physical Access Control Systems or Devices AND guards}
  2. Maintain physical access audit logs for defined entry or exit points
  3. Control access to areas within the facility designated as publicly accessible by implementing the following controls: {Organization Listed Physical Access Controls}
  4. Escort visitors and control visitor activity within restricted access area where the information system resides
  5. Secure keys, combinations, and other physical access devices
  6. Inventory physical access devices at least annually
  7. Change combinations and keys at least annually or earlier as required by a security relevant event and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

## Access Control for Transmission Medium [PE-4]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} shall:

Control physical access to organization system distribution and transmission lines within organizational facilities using {Insert Organization Security Control Language if applicable}.

## Access Control for Output Devices [PE-5]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} shall:

Control physical access to output from defined output devices to prevent unauthorized individuals from obtaining the output.

## Monitoring Physical Access [PE-6]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} shall do the following:

1. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents
2. Review physical access logs at least monthly and upon occurrence of defined events or potential indications of events
3. Coordinate results of reviews and investigations with the organizational incident response capability

## Visitor Access Records [PE-8]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} shall ensure the following:

1. Maintain visitor access records to the facility where the system resides for a minimum of one (1) year
2. Review visitor access records at least monthly
3. Report anomalies in visitor access records to {Insert Individual, Role, or Team Name}.

## Power Equipment and Power Cabling [PE-9]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} must protect power equipment and power cabling for the system from damage and destruction.

## Emergency Shutoff [PE-10]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} shall ensure the following:

1. Provide the capability of shutting off power to {Insert System Name or Individual System Components} in emergency situations
2. Place emergency shutoff switches or devices in {Organization-defined locations (e.g., Near more than one egress point of the IT Area)} and ensures it is labeled and protected by a cover to prevent accidental shut-off to facilitate access for authorized personnel
3. Protect emergency power shutoff capability from unauthorized activation

## Emergency Power [PE-11]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} shall:

Provide an uninterruptible power supply to facilitate {Organization-defined Process of orderly shutdown or Transition to Alternate Power} in the event of a primary power source loss.

## Emergency Lighting [PE-12]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} must:

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

## Fire Protection [PE-13]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} must:

Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

## Temperature and Humidity Controls [PE-14]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} must:

1. Maintain consistent with [American Society of Heating, Refrigerating and Air-conditioning Engineers (ASLR) document entitled Thermal Guidelines for Data Processing Environments] levels within the facility where the system resides at organization-defined acceptable levels
2. Monitor environmental control levels continuously.

## Water Damage Protection [PE-15]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} must:

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

## Delivery and Removal [PE-16]

This control is inherited from {IaaS/PaaS Provider}. Exact control language can be found at {StateRAMP Package ID}

or

{Insert Company Name} must:

1. Authorize and control all information system components entering and exiting the facility
2. Maintain records of the system components

## Alternate Work Site [PE-17]

To facilitate employees working at alternate sites: [PE-17 (a)]

* {Insert Company Name} configures all laptops to automatically connect to {Organization-defined} VPN when not already connected to {Organization-defined} network.
* {Insert Company Name} trains all employees to be aware of their surrounding while working and to meet the following conditions to prevent unauthorized access to the {Insert Product Name} Information System: [PE-17 (b)]
  + Unless otherwise approved, employees are only permitted to work at alternative work sites located in the United States.
  + Employees may not disable any security software or configurations established on their company issued device
  + Employees must connect company property to {Organization-defined} VPN at alternate work sites over an encrypted connection
  + Employees must take precautions to prevent shoulder surfing when working in public areas
  + Employees 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} ensures that the operating system, Group Policy Objects, VPN, and security software on all {Organization-defined} laptops are continuously updated, DNS filtering is operational, and monitors device connection information including location. [PE-17 (c)]
* {Insert Company Name} provides each corporate team member with a {Organization-defined} account which can be utilized to report a security incident to the Information Security Team by instant message, {Organization-defined} channel, or voice call. [PE-17 (d)]