Insert Logo Here

Organization Name

Security Policy

Physical & Environmental Protection

Version 1.0

April 6, 2021

Proprietary and Confidential

For Authorized Use Only

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 4/6/2021 | 1.0 | Published PE Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68593935)

[2 Purpose 1](#_Toc68593936)

[3 Scope 1](#_Toc68593937)

[4 Roles and Responsibilities 1](#_Toc68593938)

[5 Management Commitment 2](#_Toc68593939)

[6 Authority 3](#_Toc68593940)

[7 Compliance 3](#_Toc68593941)

[8 Policy Requirements 4](#_Toc68593942)

[8.1 Physical and Environmental Protection Policies and Procedures 4](#_Toc68593943)

[8.2 Physical Access Authorizations 4](#_Toc68593944)

[8.3 Physical Access Control 4](#_Toc68593945)

[8.4 Access Control for Transmission Medium 5](#_Toc68593946)

[8.5 Access Control for Output Devices 5](#_Toc68593947)

[8.6 Monitoring Physical Access 5](#_Toc68593948)

[8.7 Visitor Access Records 5](#_Toc68593949)

[8.8 Power Equipment and Power Cabling 5](#_Toc68593950)

[8.9 Emergency Shutoff 5](#_Toc68593951)

[8.10 Emergency Power 5](#_Toc68593952)

[8.11 Emergency Lighting 5](#_Toc68593953)

[8.12 Fire Protection 5](#_Toc68593954)

[8.13 Temperature and Humidity Controls 6](#_Toc68593955)

[8.14 Water Damage Protection 6](#_Toc68593956)

[8.15 Delivery and Removal 6](#_Toc68593957)

[8.16 Alternate Work Site 6](#_Toc68593958)

# Introduction

Organization Name has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by Organization 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 4.

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of Organization 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 Organization Name employees, contractors, third parties, and others who have access to company and customer confidential information within Organization Name systems and facilities.

# Roles and Responsibilities

These policies apply to all Organization Name employees, contractors, business partners, third parties, and others who need or have access to Organization Name systems and our customer's confidential information.

| **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 Organization 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. |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | 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 Manager | 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 Administrator | Responsible for conducting information system security Administration activities. |
|  | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures |
|  | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

Organization 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 Organization Name system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the Organization 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/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
8. 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 Organization 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 annually by an external vendor 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 physical and environmental security requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the Organization Name information systems.

## Physical and Environmental Protection Policies and Procedures

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 physical and environmental protection controls have been developed, documented, and disseminated to all applicable personnel.

The Information Owner will review and update the *Physical and Environmental Protection Policy* every three (3) years and the procedure(s) at least annually or any time there are significant changes in software or security. Updates must be made to keep the policy and procedure(s) in alignment with Organization Name overall business goals and risk position. Any updates, improvements, or suggestions regarding the *Physical and Environmental Protection Policy* and/or procedure(s) must be sent to the Information Owner.

## Physical Access Authorizations

For the facilities housing 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. The facility access list shall be reviewed and authorized at least annually and personnel no longer requiring access shall be removed from the authorized access list. Authorization credentials for facility access will be issued to those individuals with appropriate access clearance.

## Physical Access Control

For the facilities housing the information system, physical access authorizations are enforced for all physical access points, including designated entry and exit points, at the facility. Physical security shall be enforced through verifying individual access authorizations before access is granted to the facility and controlling entry to the facility using physical access control devices and/or guards.

Access to areas officially designated as publicly accessible are controlled in accordance with Organization Name assessment of potential risk. 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
* Visitors must be escorted to their destination and monitored
* Keys, combinations, and other physical access devices must be secured
* Physical access devices must be inventoried at least annually
* Combinations and keys must be changed at least annually and when keys are lost, combinations are compromised, or when an employee is transferred or terminated

## Access Control for Transmission Medium

For the facilities housing the information system, physical access to system distribution and transmission lines within the facilities are controlled using physical and logical access restrictions.

## Access Control for Output Devices

For the facilities housing the information system, physical access to facility output devices are controlled to prevent unauthorized individuals from obtaining the output.

## Monitoring Physical Access

For the facilities housing the information system, physical access to the facility is controlled to ensure that Organization Name can detect and respond to physical security incidents. The following physical security measures have been put in place to support this objective:

* Physical access logs are reviewed at least monthly and upon occurrence of events or potential indications of events
* Results of reviews and investigations are coordinated with Organization Name incident response capability
* Real-time physical intrusion alarms and surveillance equipment are monitored on a regular basis

## Visitor Access Records

For the facilities housing the information system, all visitor access records for the facility are reviewed at least monthly and maintained for a minimum of one (1) year.

## Power Equipment and Power Cabling

All power equipment and power cabling for the facilities housing the information system, must be protected from damage and destruction.

## Emergency Shutoff

For the facilities housing 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. Emergency shutoff switches or devices must be placed in locations that facilitate safe and easy access to authorized personnel. Additionally, emergency power shutoff capability must be protected from unauthorized activation.

## Emergency Power

For the facilities housing the information system, Organization 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.

## Emergency Lighting

Automatic emergency lighting is employed and maintained at Organization Name lighting will activate in the event of a power outage or disruption and will cover emergency exits and evacuation routes within the facility.

## Fire Protection

For the facilities housing the information system, the following fire protection measures have been put in place and must be maintained:

* Fire suppression and detection devices/systems that are supported by an independent energy source are employed and maintained
* Fire detection devices/systems that activate automatically and notify emergency responders in the event of a fire are employed
* Fire suppression devices/systems that provide automatic notification of any activation to emergency responders are employed
* An automatic fire suppression capability is employed when the facility is not staffed on a continuous basis

## Temperature and Humidity Controls

For the facilities housing the information system, the following temperature and humidity controls have been put in place and must be maintained:

* 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
* Temperature at server inlets and humidity levels by dew point are measured
* Temperature and humidity levels are monitored continuously
* Temperature and humidity monitoring method is employed that provides an alarm or notification of changes potentially harmful to personnel or equipment

## Water Damage Protection

For the facilities housing the information system, 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.

## Delivery and Removal

For the facilities housing the information system, that all components entering and exiting the facility are authorized, monitored, and controlled, and records of those items are maintained.

## Alternate Work Site

For those individuals or teams working at alternate work locations, the following security measures have been put in place:

* Employees must connect company property the corporate VPN at alternate work sites
* Assess the effectiveness of security controls at alternate work sites on an ongoing basis
* Provide a means for employees to communicate with information security personnel in case of security incidents or problems