Insert Logo Here

Organization Name

Security Policy

Media 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 MP Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68593385)

[2 Purpose 1](#_Toc68593386)

[3 Scope 1](#_Toc68593387)

[4 Roles and Responsibilities 1](#_Toc68593388)

[5 Management Commitment 2](#_Toc68593389)

[6 Authority 3](#_Toc68593390)

[7 Compliance 3](#_Toc68593391)

[8 Policy Requirements 4](#_Toc68593392)

[8.1 Media Protection Policies and Procedures 4](#_Toc68593393)

[8.2 Media Access 4](#_Toc68593394)

[8.3 Media Labeling 4](#_Toc68593395)

[8.4 Media Storage 4](#_Toc68593396)

[8.5 Media Transport 4](#_Toc68593397)

[8.6 Media Sanitization and Disposal 5](#_Toc68593398)

[8.7 Media Use 5](#_Toc68593399)

# 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 media protection 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.

## Media Protection Policies and Procedures

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

The Information Owner will review and update the *Media 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 *Media Protection Policy* and/or procedure(s) must be sent to the Information Owner.

## Media Access

Organization Name must ensure that access to digital and non-digital media is restricted to personnel with a legitimate need to know.

## Media Labeling

Information system media and information system output must be marked to indicate the distribution limitations, handling caveats, and applicable security levels (if any) of the information. No removable media is exempt from marking.

## Media Storage

All magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks are physically controlled and securely stored within access-controlled areas using encryption using a FIPS 140-2 validated encryption module for digital media and secure storage in locked cabinets or safes for non-digital media.

Additionally, automated mechanisms are used to restrict access to media storage areas and to audit access attempts and access granted. All system media shall be protected until the media is destroyed or sanitized using approved equipment, techniques, and procedures.

## Media Transport

All magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks are protected and controlled during transport outside of controlled areas using a FIPS 140-2 validated encryption module for digital media and secured in locked containers for non-digital media.

Activities associated with transport of such media are restricted to authorized personnel and must be documented using the trusted carrier’s official custody record (examples include the United States Postal Service (USPS) using Registered Mail, FedEx, or UPS).

Cryptographic mechanisms shall be used to protect the confidentiality and integrity of information stored on digital media and accountability for system media will be maintained during transport outside of controlled areas.

## Media Sanitization and Disposal

All system media, both digital and non-digital, will be sanitized prior to disposal, release out of organizational control, or release for reuse. Sanitization mechanisms are used on the media that have the strength and integrity commensurate with the classification or sensitivity of the information on the media and all sanitization equipment and procedures are tested at least annually to verify that the intended sanitation is being achieved.

## Media Use

The use of external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks are restricted or prohibited on the system using safeguards. The use of portable storage devices are prohibited in organizational information systems when such devices have no identifiable owner.