

{Insert CompanY Name}

Security Procedures

Media Protection [MP]

**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 [MP-1] ............................................................................................................ 4

8.1 Media Access [MP-2] ....................................................................................................................... 4

8.2 Media Marking, Storage, and Transport [MP-3, MP-4, MP-5] ......................................................... 4

8.3 Media Sanitization [MP-6] ................................................................................................................ 6

8.4 Media Use [MP-7] ............................................................................................................................ 6

# 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.

# Procedural Requirements [MP-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.

## Media Access [MP-2]

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

or

Restrict access to {Insert Organization-define Media. (e.g., all types of digital and/or non-digital media containing sensitive information)} to {Organization-defined Teams or Roles}.

## Media Marking, Storage, and Transport [MP-3, MP-4, MP-5]

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

or

{Insert Company Name} shall require the following:

* Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information
* Exempt no removable media types from marking if the media remain within the organization-defined security safeguards not applicable [MP-3]

{Insert Company Name} shall require the following:

* Physically control and securely store all types of digital and non-digital media with sensitive information within organization-defined Authorization Boundary
* Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures [MP-4]

{Insert Company Name} shall require the following:

* Protect and control all media with sensitive information during transport outside of controlled areas using {Organization-defined Control Language} prior to leaving secure/controlled environment
* Maintain accountability for system media during transport outside of controlled areas
* Document activities associated with the transport of system media
* Restrict the activities associated with the transport of system media to authorized personnel [MP-5]

## Media Sanitization [MP-6]

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

or

{Insert Company Name} shall require the following:

* Sanitize techniques and procedures [IAW NIST SP 800-88 Section 4: Reuse and Disposal of Storage Media and Hardware] prior to disposal, release out of organizational control, or release for reuse using {Organization-defined Sanitization Procedures}
* Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information

## Media Use [MP-7]

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

or

{Insert Company Name} shall require the following:

* {Select: Restrict or Prohibit} the use of {List Types of System Media} on {Defined Systems or System Components} using {Organizational Control Language}
* Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner