

GovRAMP

{Insert Company Name}

Security Policy

Media Protection

**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

[Document Revision History 1](#_Toc196400990)

[Table of Contents 2](#_Toc196400991)

[1 Introduction 3](#_Toc196400992)

[2 Purpose 3](#_Toc196400993)

[3 Scope 3](#_Toc196400994)

[4 Roles and Responsibilities 3](#_Toc196400995)

[5 Management Commitment 4](#_Toc196400996)

[6 Authority 5](#_Toc196400997)

[7 Compliance 5](#_Toc196400998)

[8 Policy Requirements 5](#_Toc196400999)

[8.1 Media Protection Policies and Procedures [MP-1] 5](#_Toc196401000)

[8.2 Media Access [MP-2] 6](#_Toc196401001)

[8.3 Media Marking [MP-3] 6](#_Toc196401002)

[8.4 Media Storage [MP-4] 6](#_Toc196401003)

[8.5 Media Transport [MP-5] 6](#_Toc196401004)

[8.6 Media Sanitization [MP-6, {MP-6 (1-3) High Only}] 6](#_Toc196401005)

[8.7 Media Use [MP-7] 7](#_Toc196401006)

# 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 Media Protection 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 Media Protection 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. |
|  | 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 Media Protection 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}.

8.1 Media Protection Policies and Procedures [MP-1]

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 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: [MP-1 (a)]

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

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

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

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

8.2 Media Access [MP-2]

{Insert Company Name} must ensure that access to digital and non-digital media is restricted from all personnel without a legitimate need to know. [MP-2]

8.3 Media Marking [MP-3]

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. [MP-3 (c)] No removable media is exempt from marking. [MP-3 (b)]

8.4 Media Storage [MP-4]

All magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks must be physically controlled and securely stored within access-controlled areas using a FIPS 140-2 validated encryption module for digital media and secure storage in locked cabinets or safes for non-digital media. [MP-4 (a)]

Additionally, mechanisms must be 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 following NIST SP 800-88 Media Sanitization. [MP-4 (b)]

8.5 Media Transport [MP-5]

All magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks must be 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. [MP-5 (a)]

Activities associated with transport of such media are restricted to authorized personnel [MP-5 (d)] 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). [MP-5 (c)]

FIPS 140-2 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. [MP-5 (b)]

8.6 Media Sanitization [MP-6, {MP-6 (1-3) High Only}]

All system media, both digital and non-digital, must be sanitized prior to disposal, release out of organizational control, or release for reuse in accordance with NIST SP 800-88 Section 4. [MP-6 (a)] Sanitization mechanisms must be on the media that have the strength and integrity commensurate with the classification or sensitivity of the information on the media. [MP-6 (b)]

**For high impact systems only:**

{Insert Company Name} must:

* Review, approve, track, document, and verify media sanitization and disposal actions. [MP-6 (1)]
* Test sanitization equipment and procedures at least semi-annually to ensure that the intended sanitization is being achieved [MP-6 (2)]
* Apply nondestructive sanitization techniques to any new portable storage device prior to connecting such devices to the system in order to remove any potential malicious code or if the device is procured from an untrustworthy source. [MP-6 (3)]

8.7 Media Use [MP-7]

The use of external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks, and other similar media are prohibited on {Insert Company Name} systems using safeguards unless the employee, role, or department has a documented exception. [MP-7 (a)]

The use of portable storage devices is prohibited in organizational systems when such devices have no identifiable owner. [MP-7 (b)]