**Media Protection (MP)**

**MP-1: Media Protection Policy and Procedures**

NIST SP 800-53 Objective: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and

b. Reviews and updates the current:

1. Media protection policy [*Assignment: organization-defined frequency*]; and

2. Media protection procedures [*Assignment: organization-defined frequency*].

Control Translation: Ensure media protection policy and procedures are in place.

Notes: The organizational risk management strategy is a key factor in the development of the media protection policy. Related control: PM-9. This control can be applied at the General level.

How to test and evaluate: Examine SSP and Media Protection Policy (if available) and verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency.

Technology specific: General

**MP-2: Media Access**

NIST SP 800-53 Objective: The organization restricts access to [*Assignment: organization-defined types of digital and/or non-digital media*] to [*Assignment: organization-defined personnel or roles*].

Control Translation: Ensure media protection policy and procedures employ media access restrictions.

Notes: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.

How to test and evaluate: Examine SSP and Media Protection Policy (if available) and verify that the policy and procedures indicate that media access restrictions are in place for both digital and non-digital. Note what types of digital and non-digital media are restricted and personnel/roles that are restricted from access.

Technology specific: Per datacenter

**MP-3: Media Marking**

NIST SP 800-53 Objective: The organization:

a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempts [*Assignment: organization-defined types of information system media*] from marking as long as the media remain within [*Assignment: organization-defined controlled areas*].

Control Translation: Ensure media protection policy and procedures have media marking in place.

Notes: The term *security marking* refers to the application/use of human-readable security attributes. The term *security labeling* refers to the application/use of security attributes with regard to internal data structures within information systems (see AC-16). Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable.

Notes: Marking of information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: AC-16, PL-2, RA-3.

How to test and evaluate: Examine SSP and Media Protection Policy (if available) and verify that the policy and procedures indicate that media marking is in place for both digital and non-digital. Note how digital and non-digital media are marked (e.g., indicating distribution limitations, handling caveats, security markings, etc.). Indicate if there are any exemptions to media marking for digital or non-digital media in controlled areas.

Technology specific: Per datacenter

**MP-4: Media Storage**

NIST SP 800-53 Objective: The organization:

a. Physically controls and securely stores [*Assignment: organization-defined types of digital and/or non-digital media*] within [*Assignment: organization-defined controlled areas*]; and

b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Control Translation: Ensure media protection policy and procedures indicate that media storage mechanism is in place.

Notes: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems.

Notes: For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection. Related controls: CP-6, CP-9, MP-2, MP-7, PE-3.

How to test and evaluate: Examine SSP and Media Protection Policy (if available) and verify that the policy and procedures indicate that media storage is in place for both digital and non-digital. Note what type of media storage is implemented. Verify if it’s in a controlled/caged area with key pad or proximity badge reader for controlled access.

Technology specific: Per datacenter

**MP-5: Media Transport**

NIST SP 800-53 Objective: The organization:

a. Protects and controls [*Assignment: organization-defined types of information system media*] during transport outside of controlled areas using [*Assignment: organization-defined security safeguards*];

b. Maintains accountability for information system media during transport outside of controlled areas;

c. Documents activities associated with the transport of information system media; and

d. Restricts the activities associated with the transport of information system media to authorized personnel.

Control Translation: Ensure media protection policy and procedures indicate that media transport mechanism is in place.

Notes: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.

Notes: Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records. Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.

How to test and evaluate: Examine SSP and Media Protection Policy (if available) and verify that the policy and procedures indicate that media transport mechanism is in place. Note how media is protected during transport, how accountability maintained, ensure activities are documented, and who is responsible for these activities.

Technology specific: Per datacenter

**MP-6: Media Sanitization**

NIST SP 800-53 Objective: The organization:

a. Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and

b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Control Translation: Ensure media protection policy and procedures indicate that media sanitization mechanism is in place.

Notes: This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization.

Notes: Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. Related controls: MA-2, MA-4, RA-3, SC-4.

How to test and evaluate: Examine SSP and Media Protection Policy (if available) and verify that the policy and procedures indicate that media sanitization mechanism is in place. Verify how media is sanitized or sanitization techniques before it is released for disposal. Also, note if there is a tracking mechanism in place to document media being sanitized. Interview and note who is responsible for the sanitization and disposal activities.

Technology specific: Per datacenter

**MP-7: Media Use**

NIST SP 800-53 Objective: The organization [*Selection: restricts; prohibits*] the use of [*Assignment: organization-defined types of information system media*] on [*Assignment: organization-defined information systems or system components*] using [*Assignment: organization-defined security safeguards*].

Control Translation: Ensure media protection policy and procedures indicate safeguards are in place for media use.

Notes: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned.

Notes: Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices. Related controls: AC-19, PL-4.

How to test and evaluate: Examine SSP and Media Protection Policy (if available) and verify that the policy and procedures indicate that media use restrictions are in place. Verify what type of media (digital and non-digital) is restricted and what safeguards are in place to control restrictions. Note if portable devices are restricted.

Technology specific: Per datacenter