| Control Identifier | Control (or Control Enhancement) Name | Control Text | Discussion | Related Controls | Data Collection | Evidence Detail | Finding | Dispostion | Threat(s) | Vulnerability Description | Mitigating Factors or Compensatory Controls in place | Likelihood | Impact | Overall Risk | Risk Explanation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| MP-1 | Policy and Procedures | a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:<br>1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that:<br>(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and<br>2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;<br>b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and<br>c. Review and update the current media protection:<br>1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and<br>2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. | Media protection policy and procedures address the controls in the MP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of media protection policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure. | PM-9, PS-8, SI-12. | Interview | Director of IT, Frank Davis | No media protection policy or procedures were available. | Not In Place | Unauthorized access | No documented processes or policies. | Tribal knowledge in place. | 5 | 5 | 25 | Staff do not know what expectations or standards are and no process around media protection, storage, sanitization is documented, so may not be done properly.<br>Without standards and policy, no process can be repeated consistently and staff will develop their own individual processes. |
| MP-2 | Media Access | Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles]. | System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers is an example of restricting access to non-digital media. Limiting access to the design specifications stored on compact discs in the media library to individuals on the system development team is an example of restricting access to digital media. | AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SC-34, SI-12. | Interview | Director of IT, Frank Davis<br>Network Engineer, James Martin | USB drives are not automounted.<br>All sensitive data is protected through access controls and database access is logged.<br>DLP solution "name" is implemented and blocking exfil. | In Place | | | | | | 0 | CONTROL IN PLACE |
| MP-3 | Media Marking | a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and<br>b. Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas]. | Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Controlled unclassified information is defined by the National Archives and Records Administration along with the appropriate safeguarding and dissemination requirements for such information and is codified in 32 CFR 2002. Security markings are generally not required for media that contains information determined by organizations to be in the public domain or to be publicly releasable. Some organizations may require markings for public information indicating that the information is publicly releasable. System media marking reflects applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. | AC-16, CP-9, MP-5, PE-22, SI-12. | Interview | Director of IT, Frank Davis<br>Network Engineer, James Martin | Reviewed documentation of identified media for marking (covid data, financials). Covid data had marking. Financial data did not have marking consistently. | Partially In Place | Data Loss/Information Disclosure | Without media marking, financial data could be disseminated to unathorized parties. | None | 2 | 8 | 16 | Financial data isn't disclosed often by accident but when it is, it has a negative impact of moral and investor confidence |
| MP-4 | Media Storage | a. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and<br>b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures. | System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library. The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or have limited adverse impacts on organizations, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection. | AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SC-34, SI-12. | Interview | Director of IT, Frank Davis<br>Network Engineer, James Martin | No control or governance around thumb drive usage and storage. | Not In Place | Data modification/ destruction/ corruption | Malware could be brought into the environment and insider threat could steal data. | USB Drive automounts disabled. | 5 | 5 | 25 | Loss of IP and introduction of malicious USB could introduce massive issues. |
| MP-5 | Media Transport | a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls];<br>b. Maintain accountability for system media during transport outside of controlled areas;<br>c. Document activities associated with the transport of system media; and<br>d. Restrict the activities associated with the transport of system media to authorized personnel. | System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), compact discs, and digital versatile discs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport. Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining 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 system media in accordance with organizational assessments of risk. Organizations maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records. | AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28, SC-34. | Interview | Director of IT, Frank Davis<br>Network Engineer, James Martin | We don't allow people to travel with data. We use cloud storage and have ppl access it from the cloud. Any system that is sent out for maintenance or repair has sensitive data wiped before being sent. | In Place | | | | | | 0 | CONTROL IN PLACE |
| MP-6 | Media Sanitization | a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and<br>b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. | Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether or not the media is considered removable. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, 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. Organizations use discretion on the employment of approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media that contains classified information. NARA policies control the sanitization process for controlled unclassified information. | AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11. | Tested | Reviewed audit records of HDD destroyed. 1 was recent but other 2 were 3 years old. | Sanitization is happening but inconsistently documented. | Partially In Place | Data Loss/Information Disclosure | Without record keeping, there is no assurance of proper sanitization. New people could take over process and result in it not being done. | Tribal knowledge process and small IT team with one guy that stated he consistently does it. | 2 | 8 | 16 | There is no assurance of proper sanitization. Tribal knowledge process. A new person may not know and if theft occurred, there would be no assurance of controlled data. |
| MP-7 | Media Use | a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and<br>b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner. | System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, compact discs, digital versatile discs, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to MP-2, which restricts user access to media, MP-7 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations use technical and nontechnical controls to restrict the use of 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 or 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 devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, such as by prohibiting the use of writeable, portable storage devices and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for storage devices reduces the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices. | AC-19, AC-20, PL-4, PM-12, SC-34, SC-41. | Interview | Director of IT, Frank Davis<br>Network Engineer, James Martin | USB Automounting is the only control in place. No documented policy or procedures. | In Place | | | | | | 0 | CONTROL IN PLACE |
| MP-8 | Media Downgrading | a. Establish [Assignment: organization-defined system media downgrading process] that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information;<br>b. Verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;<br>c. Identify [Assignment: organization-defined system media requiring downgrading]; and<br>d. Downgrade the identified system media using the established process. | Media downgrading applies to digital and non-digital media subject to release outside of the organization, whether the media is considered removable or not. When applied to system media, the downgrading process removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading ensures that empty space on the media is devoid of information. | None. | Interview | Director of IT, Frank Davis<br>Network Engineer, James Martin | There is no process or requirement for media downgrading. | N/A | | | | | | 0 | NOT APPLICABLE |