

For High-Impact Information Systems

FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

MP-1.1 - Examine media protection policy and procedures; other relevant documents or records, and

Interview organizational personnel with information system media protection responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents media protection policy and procedures.				
(ii)	The organization disseminates media protection policy and procedures to appropriate elements within the organization.				
(iii)	Responsible parties within the organization periodically review media protection policy and procedures.				
(iv)	The organization updates media protection policy and procedures when organizational review indicates updates are required.				

MP-1.2 - Examine media protection policy and procedures; other relevant documents or records, and

Interview organizational personnel with information system media protection responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The media protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance.				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(ii)	The media protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance.				
(iii)	The media protection procedures address all areas identified in the media protection policy and address achieving policy-compliant implementations of all associated security controls.				

MP-2 MEDIA ACCESS - The organization restricts access to information system media to authorized individuals.

MP-2.1 - Examine information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records, **and**

Interview organizational personnel with information system media protection responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization restricts access to information system media to authorized users.				

MP-2(1).1 - Examine information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control devices; access control records; audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization employs automated mechanisms to restrict access to media storage areas.				
(ii)	The organization employs automated mechanisms to audit access attempts and access granted.				

and

Test automated mechanisms implementing access restrictions to media storage areas to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Validate that automated mechanisms restrict access to media storage areas.				

MP-3 MEDIA LABELING - The organization: (i) affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) exempts specific media types or hardware components from labeling so long as they remain within the organizations protected environment.

MP-3.1 - Examine information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; information system security plan (for the definition of controlled areas for the organization); removable storage media and information system output; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines its protected environment for media labeling requirements.				
(ii)	The organization identifies media types and hardware components that are exempted from external labeling requirements.				
(iii)	The organization exempts the organization-defined list of media types and hardware components from labeling so long as they remain within the organization-defined protected environment.				
(iv)	The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information.				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	.				

MP-4 MEDIA STORAGE - The organization physically controls and securely stores information system media within controlled areas.

MP-4.1 - Examine information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan (for the definition of controlled areas for the organization); information system media; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines controlled areas for information system media.				
(ii)	The organization selects and documents the media and associated information contained on that media requiring physical protection in accordance with an organizational assessment of risk.				
(iii)	The organization defines the specific measures used to protect the selected media and information contained on that media.				
(iv)	The organization physically controls and securely stores information system media within controlled areas.				
(v)	The organization protects information system media commensurate with the FIPS 199 security categorization of the information contained on the media.				

MP-5 MEDIA TRANSPORT - The organization protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.

MP-5.1 - Examine information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan (for definition of controlled areas for the organization); list of organization-defined personnel authorized to transport information system media outside of

controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies personnel authorized to transport information system media outside of controlled areas.				
(ii)	The organization controls information system media during transport outside of controlled areas.				
(iii)	The organization restricts the activities associated with transport of information system media to authorized personnel.				

MP-5(1).1 - Examine information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan (for the definition of controlled areas for the organization); information system media transport records; audit records; other relevant documents or records, **and**

Interview organizational personnel with information system media transport responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines security measures (e.g., locked container, cryptography) for information system media transported outside of controlled areas.				
(ii)	The organization protects digital and non-digital media during transport outside of controlled areas using the organization-defined security measures.				

MP-5(2).1 - Examine information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan (for organization-defined system of records for media transport); information system media transport records; audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines a system of records for documenting activities associated with the transport of information system media.				
(ii)	The organization documents, where appropriate, activities associated with the transport of information system media using the organization-defined system of records.				

MP-6 MEDIA SANITIZATION AND DISPOSAL - The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse.

MP-6.1 - Examine information system media protection policy; procedures addressing media sanitization and disposal; NIST Special Publication 800-88; media sanitization records; audit records; other relevant documents or records, **and**

Interview organizational personnel with information system media sanitization responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the process.				
(ii)	The organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse.				
(iii)	Information system media sanitation is consistent with NIST Special Publication 800-88.				