





A Media Protection Policy defines how an organization safeguards all forms of media including digital and physical. The primary purpose of this policy is to prevent unauthorized access, use, disclosure, or modification of any and all sensitive information that might be stored on or transferred via either digital or physical means. This policy is crucial for mitigating risks associated with media handling.

Recommended Actions:

-  Encrypt or restrict access to sensitive files (on USBs, CDs, phones, cloud)
-  Don't let just anyone take data off your systems
-  Safely destroy old drives (shred, wipe)
-  Label media if it contains sensitive information

The following template may be used to help with the creation and implementation of your own policies and procedures.

For more information related to Access Control and other fundamental areas please visit the following link:

[CMMC Assessment Guide Level 1](#)

- MP.L1-b.1.vii – Media Disposal [FCI Data]

Policy #:	Title:	Effective Date:
	Media Protection Policy	

PURPOSE

To ensure that Information Technology (IT) controls access to and disposes of media resources in compliance with IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – Media Protection (MP), NIST SP 800-12, NIST SP 800-56, NIST SP 800-57, NIST SP 800-60, NIST SP 800-88, NIST SP 800-100, NIST SP 800-111;
NIST Federal Information Processing Standards (FIPS) 199

POLICY

This policy is applicable to all departments and users of IT resources and assets.

1. MEDIA ACCESS:

IT through direction from departments shall:

- a. Restrict access to _____
to _____.
- b. Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.

2. MEDIA STORAGE

IT Department shall:

- a. Specify staff to physically control and securely store media within defined controlled areas.
- b. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

3. MEDIA TRANSPORT

IT Department Shall:

- a. Protect and control media during transport outside of controlled areas.
- b. Maintain accountability for information system media during transport outside of controlled areas.

- c. Document activities associated with the transport of information system media.
- d. Restrict the activities associated with the transport of information system media to authorized personnel.

4. MEDIA SANITIZATION

IT Department shall:

- a. Sanitize prior to disposal, release out of organizational control, or release for reuse using _____ in accordance with applicable federal and organizational standards and policies.
- b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

5. MEDIA USE

IT Department shall:

Prohibit the use of _____ on _____ owned equipment using unapproved security safeguards.

COMPLIANCE

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED

Date Issued:	
Date Reviewed:	