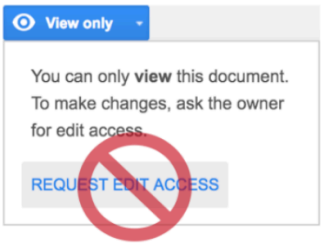
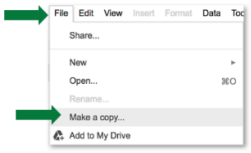
Strike Graph

Media Protection Policy Template



How to use this template:

This is a view-only file and cannot be edited. **Create your own copy** of this template to edit. In the menu, click **File > Make a copy...**



Strike Graph

Strike Graph Notes:

This Media Protection policy template sets the rules for how your organization controls, stores, transports, sanitizes, and disposes of media containing sensitive information. It's intentionally straightforward: anywhere you see text in brackets, that's a cue to customize the wording to fit your own departments, media types, and internal terminology before publishing.

Policy #:	Title:	Effective Date:
x.xxx	Media Protection Policy	MM/DD/YY

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:

Strike Graph Notes:
Use the brackets to name the specific media you care about most (e.g., USB drives, backup tapes, laptops, printed CUI) and the roles allowed to access them (e.g., Storage Admins, Records Management, specific business units). Reference your asset inventory so the list is realistic. Auditors will check that this matches how you really operate and that review dates are current.

IT through direction from departments shall:

a. Restrict access to [entity defined types of digital and/or non-digital media] to [entity identified staff].

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:

Strike Graph Notes:
Reference your chosen standard explicitly in the bracket, such as “NIST SP 800-88, latest revision” plus any internal SOP or vendor process you actually use. Clarify whether IT, a destruction vendor, or Records Management is responsible. Keep disposal logs and certificates of destruction aligned with this wording and ensure dates issued/reviewed reflect when you last validated your process.

IT through direction from departments shall:

a. Sanitize prior to disposal, release out of organizational control, or release for reuse using [entity specified standard] 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:

Strike Graph Notes:
Use the bracket to spell out which media are restricted (e.g., personal USB drives, non-encrypted external disks, cloud storage not on an approved list). Tie this to your technical controls (DLP, endpoint controls) and HR/disciplinary process. Make sure the prohibition here is consistent with Acceptable Use, and that the policy’s effective and review dates match your actual enforcement timeline.

IT through direction from departments shall:

a. Prohibit the use of [entity defined types of information system media] on [entity] 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:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY