# Media Protection Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The quality and integrity of [Company Name’s] media protection mechanisms allow information to be provided a greater level of security than can be achieved with system based protection mechanisms alone. Without media protection mechanisms, the potential exists that [Company Name]’s information assets could be exposed to an unnecessarily high level of risk, particularly in circumstances where that information is taken out of the information system.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

The Media Protection Policy applies to all employees of [Company Name], including all temporary or contract workers. Specifically, it applies to all email accounts provided by [Company Name] and all email transmissions made over [Company Name] networks and network services.

* Removable magnetic media including external hard disk drives, external devices containing hard disk drives, floppy disks, and magnetic tape.
* Removable flash-based media including thumb drives, digital media players, digital cameras, and smart phones / cell phones.
* Optical media including DVDs and CDs.
* Paper and other printable materials.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. All privileged information when stored out of system (via information media) will be protected by media protection mechanisms to ensure the highest levels of security. Non-privileged information will be protected to ensure the highest levels of integrity and availability.
2. Where information is transferred to media that media shall be stored securely within a controlled area and access to that controlled area shall be physically restricted to authorized personnel. Further, the mechanisms that enforce those access restrictions shall collect access information and shall include the ability to audit access attempts.
3. When content from the information system is output to some form of media, that content and media must be handled and stored in a secure manner.
4. When information system media is transported, it shall be done so in a secure manner and only by personnel specifically authorized to do so. Further, all such transportation shall be documented.
5. Once information system media is no longer needed to store or transport system information, it must be completely sanitized before reuse or destroyed before retirement.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

Restrict access to media and media output devices:

* + - * + Where possible, protect media output devices from inappropriate access by placing them in secure locations.
        + Control access to media output devices placed in secure locations by requiring identified and authenticated access to those locations.
        + Where media output devices cannot be placed in secure locations, configure those devices to output media only when attended.
        + Disable local media output devices that cannot be configured to only output media when attended.
        + Place all media in locked cabinets and place those cabinets in controlled access locations.
        + Maintain a media access log.

Transport media that contains data in a secure fashion:

* + - * + Before allowing media to be transported, verify that a copy of the data stored on the media exists elsewhere.
        + Place all media in a locked container that will protect it from environmental and man-made threats.
        + Maintain a media transportation log.

Positively dispose of media that is no longer required:

* + - * + Where digital media has reached the end of its lifespan, the media must be physically destroyed and rendered unusable before being discarded.
        + Where non-digital media has reached the end of its usability, the media must be physically destroyed and rendered illegible and unusable before being discarded.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.