This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the outlined image.

Storage Media Security Policy Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously.
- Enter “<organization name>” in the Find text box.
- Enter your organization’s full name in the “Replace” text box.
- Click “More”, and make sure “Match case” is ticked.
- Click “Replace All”.
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Choose Classification

VERSION <1.0>

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This policy aims to define the cybersecurity requirements related to the secure use and disposal of storage media used with <organization's name>'s systems, data and information, in order to achieve the main objective of this policy which is minimizing cybersecurity risks to preserve confidentiality, integrity and availability.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy covers all <organization name>'s information and technology assets and applies to all personnel (employees and contractors) in <organization name>.

Policy Statements

1. General Statements

1-1 The <organization name> must ensure the controlled use of storage media devices utilized to store and transfer information by personnel who have access to information and technology assets at <organization name>.

1-2 <organization name> must define what is considered as removable media and which of these can be connected to an information system, computer, or network to provide data storage, such as:

- Magnetic (e.g., spinning disk drives, tapes).
- Optical (e.g., optical drives such as CD-R, DVD-R, Blu-ray), and magneto-optical.
- Semiconductor (e.g., SSD, flash drives, persistent memory devices).

1-3 <organization name> must prohibit the use of all removable media devices unless a valid business case for its use is provided.

1-4 <organization name> must design and implement a formal process for approving the use of removable media.

1-5 <organization name> must physically control and securely store storage media devices within <organization name>.

1-6 <organization name> must protect storage media devices until the media are disposed or sanitized using approved equipment, techniques, and procedures, in alignment with the <organization name>' Secure Disposal Policy.

1-7 <organization name> must restrict the use and provide secure handling of external storage media.

2. Media Access

2-1 Access to the following types of storage media must be restricted in alignment with Asset Management Policy:

- <Organization defined media type 01 (e.g., backup tape)>
- <Organization defined media type 02 (e.g., server storage media)>
- <Organization defined media type 03 (e.g., network storage)>

2-2 The distribution limitations, handling caveats, and applicable security markings of storage media must be applied.

3. Media Storage

3-1 Personnel must be appointed to physically control and securely store media within defined controlled areas.

3-2 Protection of storage media until the media are destroyed or sanitized using equipment approval processes, definition of media handling procedures and approved protection techniques must be ensured.

4. Media Transport

4-1 Media must be protected and controlled, during transport outside of controlled areas.

4-2 Accountability for storage media during transport outside of controlled areas must be maintained.

4-3 Activities associated with the transport of storage media must be documented and must be restricted to authorized personnel.

4-4 <organization name> must establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media.

4-5 <organization name> must review and update the media transportation related policies and procedures at least annually.

5. Media Sanitization

5-1 <organization name> must sanitize storage media prior to its disposal, releasing it out of organizational control or releasing it for reuse using Storage Security Standard in accordance with applicable regulatory and organizational standards and policies.

5-2 Sanitization mechanisms with the strength and integrity commensurate with the classification of the information must be applied.

6. Media Use

6-1 <organization name> must prohibit the use of <organization name> defined types of storage media on equipment owned by <organization name> using unapproved security safeguards.

Roles and Responsibilities

1- **Policy Owner:** <head of cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

3- **Policy Implementation and Execution:** <information technology function> and <cybersecurity function>

4- **Policy Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- <Head of cybersecurity function> will ensure the compliance of <organization name> with this policy on a regular basis.

2- All personnel of <organization name> must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action according to <organization name>'s procedures.