Electronic Data Storage Media Handling Policy

# Template

This is an example policy. Please ensure you update this policy template so that it’s suitable for your organisation.

## Function

This policy supports the ‘Information Security Policy’. This document forms part of our Information Security Management System. It outlines the rules with which we store, handle and transport physical removable media. This includes the security measures employed around the use of portable devices, such as memory sticks, laptops and smartphones. The policy also identifies how to dispose of media securely at the end of its lifecycle.

## Scope

### Employees

This policy applies to all who use <Organisation>‘s media:

* employees
* contractors
* volunteers
* third party employees

### IT Assets

This policy applies to all organisational IT assets.

### Documentation

The documentation will consist of a ‘Media Handling Policy’, and related procedures and guidelines. The Electronic Data Storage Media Handling (EDSMH) Policy, and all other referenced documents, will be controlled.

Version control will be to preserve the latest release and the previous version of any document. However, the previous version of the documents will be retained only for a period of 2 years for legal and knowledge preservation purposes.

### Records

Records being provided as part of the EDSMH policy will be retained for a period of 2 years. Records will be in hard copy or electronic media. The records will be owned by the system administrators and will be audited once a year.

### Distribution and Maintenance

The EDSMH policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document will be made available to those concerned. The maintenance responsibility of the document will be with the <Role>.

## Responsibility

The EDSMH policy will be implemented by the <Role>.

## Definitions

Electronic data storage media is any device that can store and or retrieve digital information. Examples of electronic data storage media include:

* floppy disks
* CDs
* computer hard drives
* DVDs
* data tapes
* memory cards

## Privacy

The EDSMH policy will be considered as ‘confidential’ and will be made available to the relevant people with proper access control. Policy changes and versions of this document will be controlled.

## Policy

The primary area of concern is the secure management of media to protect sensitive or personal information from intentional or accidental exposure or misuse. The following will be implemented:

1. Risks to information and the media it’s held on will be securely managed throughout the lifecycle of procurement, use, storage, and disposal.
2. Only authorised media will be used for managing data.
3. Media will be handled according to the highest level of sensitivity of contained information.
4. Media will be protected from theft or tampering.
5. Where there’s re-assignment or destruction of hardware and media, inventory records shall be kept current.
6. Media will be wiped when its content is no longer needed. Wiping is the process of writing data over the hard drive, so that any data stored on the drive is overwritten by the new data and may not be retrieved.
7. Media will be destroyed when it’s no longer usable. Destruction is the physical demolition of the data storage media so it’s unusable. In this case, destroyed media equipment will be:
* disintegrated
* incinerated
* pulverized
* shredded
* melted

These are specific techniques required for specific media.

1. Hard disk drives, flash drives, memory cards should be struck with a heavy object until the drive is inoperable. Scraping away recording media with a sharp object on hard disk platters is not acceptable.
2. CDs, DVDs, data tapes should be shredded or broken into pieces.

## Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the <role> and <organisation>.

Policy exceptions must describe:

* the nature of the exception
* a reasonable explanation for why the policy exception is required
* any risks created by the policy exception
* evidence of approval by all appropriate parties

## Compliance

Compliance with this policy is the responsibility of the <role>.

## Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy.

Review of this document: annually by the <role>.

Next review date: <date month year>.