# **DATA DESTRUCTION POLICY AND PROCEDURES**

Sumário

[**DATA DESTRUCTION POLICY AND PROCEDURES** 1](#_Toc108693323)

[**Introduction** 3](#_Toc108693324)

[**Scope** 3](#_Toc108693325)

[**Minium Retention Period** 3](#_Toc108693326)

[**Security Categorization** 3](#_Toc108693327)

[**Media Control** 4](#_Toc108693328)

[**Roles and Responsabilities** 4](#_Toc108693329)

[**Data Destruction Procedures** 5](#_Toc108693330)

[**Record of Data Destruction** 9](#_Toc108693331)

[**Additional Information - Tools** 9](#_Toc108693332)

## **Introduction**

This policy ver1.0 released 14 July, 2022 instructs all parties involved, including the program manager, data owner, information system owner, IT asset management team, vendors & other personnel, to adhere to the norms specified herein for safe and compliant data destruction. Key Goals of this data destruction policy ver1.0 implementation is to attain:

A data retention and destruction policy facilitates the transparent management of a company’s data. It also helps a company comply with state and federal government regulations. The government is keen on implementing data security legislation, and it’s best practice for companies to apply regulations to their operations.

Data retention and destruction policies protect a company from lawsuits and penalties that can prove costly to a business due to fines and surcharges for not complying with the law. Depending on the industry, fines can run into millions of dollars due to the sensitivity of data.

## **Scope**

The policy covers the records listed in the Information Asset Register irrespective of

the media on which they are created or held including:

* Papers;
* Digital Files (Databases, Word Documents, Power Point, spreadsheets, webpages and e-mails);
* Photographs, Scanned images and vídeos;

The records may include, but are not limited to, the following:

* Client Files;
* Contracts and Invoices;
* Registers;
* Legal advice;
* Financial accounts;
* Employee Information;
* Member information;

## **Minium Retention Period**

Unless a record has been marked for 'permanent preservation' it will only be retained

for a limited period of time. The five-year retention period applies to all records

within the category of service providers. Member and employee records will be maintained throughout employment/lease until effective termination.

## **Security Categorization**

The data destruction policy needs to define the security categorization in terms of the potential impact of events that danger the information. According to the Federal Information Processing Standard Publication 199 (FIPS 199) , “Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.” FIPS 199 defines the following security categorizations based on the Information Types and Information Standards:

* **Security categorization applied to information types:**This categorization is determined based on the impact of compromised user information and system information. So, the policy should include a provision to segregate the data in tiers based on its security categorization to allow a focused and commensurate destruction approach.
* **Security categorization for information systems:** Security categorization of information systems requires a deeper analysis of the data storage systems and also needs to consider the security categorization of the information types residing in the information systems.

## **Media Control**

**a)   Internal control:** The storage media is entirely under the organization’s internal control if it is managed by the company’s in-house IT asset management team. Media handed over to external vendors for maintenance or upgrade is also considered in the organization’s control, provided the necessary agreements are in place to secure data privacy and confidentiality. Further, “onsite” maintenance of storage media by third-party vendors like MSPs and MSSPs under the organization’s supervision also counts as internally controlled media.

**b)   External control:** The storage media permanently leaves the organization’s ownership through transactions like resell, return, and disposal for recycling. Here, the control over the storage media and underlying data, if not destroyed, changes to the new owner.

## **Roles and Responsabilities**

The data destruction policy must precisely define the roles and responsibilities to ensure data protection through its entire lifecycle. As per NIST SP 800-88, the following are some pertinent roles and responsibilities within the organization:

**a)   Chief Information Officer (CIO) -** This role owns the information assets, including data security, integrity, and privacy aspects, within the organization. The CIO (or sometimes the business unit head) defines the policies and principles for data access and usage. They also promulgate the data destruction principles as a component of the information security policy and ensure that data destruction standards are met.

**b)   Chief Information Security Officer (CISO)** – This role is responsible for crafting the vision, strategy, and plan to protect the organization’s information assets and ensure data security. The CISO role can own and shoulder the overall “data protection” charter out of the broader CIO role.

**c)    Program Manager -**This role is responsible for establishing an effective data security governance structure and organizing the resources for the program’s success.

**d)   Data Steward -**Data steward implements the principles and policies laid down by the information owner (CIO or BU head). The individual — aside from managing the data availability and quality — acts as an interface between the business unit and IT asset management team to ensure the destruction of sensitive information as necessary.

**e)   Information System Owner** **-** This role ensures the sanity of maintenance and contractual agreements to adequately protect the storage system and data as per applicable security categorization levels.

**f)    Property Management Officer** - This role is responsible for ensuring redistribution of the storage media within the organization or to external parties as applicable after data destruction.

**g)   Records Management Officer** - The records management officer maintains detailed records of all types of information and advises the information owner concerning the data retention requirements.

**h)   Privacy Officer** - The privacy officer provides counselling on privacy issues concerning the data destruction process and storage media. They also owns the responsibility of interpreting any deviations in following the protocols and subsequent impacts, including data breaches.

**i)     Users** - They are responsible for knowing the confidentiality of data they use and its safe handling to maintain the privacy standards.

**Data Destruction Procedures**  
The policy should lay down the data destruction procedure based on the optimal combination of techniques for the storage media types. NIST SP 800:88 Guidelines define a comprehensive media sanitization matrix using the Clear, Purge, and Destroy data destruction techniques

Onsite data destruction is performed using DIY data erasure software or a degausser operated by a competent technician. Sometimes, mobile shredding trucks operated by IT asset destruction (ITAD) service vendors can also perform onsite data destruction provided the logistic and financial constraints are met. In contrast, offsite data destruction can be performed using data erasure software, degausser, or shredder.

***Note:****Offsite data destruction poses inherent chain-of-custody risks to the data. Therefore, the policy should consider including an explicit provision to mandate “onsite erasure” of storage devices before the organization releases the custody to the offsite service vendor.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Storage Media** | **Clear** | **Purge** | **Destroy** |
| **Paper and microforms** | NA | NA | Shred using cross cut shredders |
| **Copier, printer, fax machine** | Device reset | Use hardware or firmware specific techniques such as rewriting, block erasure, or cryptographic erasure | Use standard physical destruction methods   * Shred * Disintegrate * Pulverize * Incinerate |
| **Routers and Switches** | Full factory reset as per OEM settings | NA | Use standard physical destruction methods |
| **Floppies** | Overwrite and verify | Degauss | Incinerate |
| **Magnetic Disks** | Overwrite and verify | Degauss | Incinerate |
| **Storage Media** | **Clear** | **Purge** | **Destroy** |
| **Reel and Cassette Format Magnetic Tapes** | Rerecord (Overwrite) | Degauss | Incinerate |
| **ATA and SCSI Hard Disk Drives. Also applicable to local external HDDs.** | Overwrite and verify | Use any of these methods:   * Overwrite EXT command * Cryptographic Erase * Use SECURE ERASE command * Degauss | Use standard physical destruction methods |
| **ATA Solid State Drives** | Overwrite and verify OR, ATA SECURITY ERASE UNIT command, if supported | * Block Erase * Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface | Use standard physical destruction methods |
| **SCSI Solid State Drives** | Overwrite and verify | * SCSI SANITIZE command * Cryptographic Erase | Use standard physical destruction methods |
| **NVM Express SSDs** | Overwrite and verify | * NVM Express Format command * Cryptographic Erase | Use standard physical destruction methods |
| **Storage Media** | **Clear** | **Purge** | **Destroy** |
| **Mobile devices** **(iOS® and Android® devices)** | Erase all contents using Factory Reset OR, Overwrite and verify | eMMC Secure Erase  or Secure Trim command for factory reset OR, Cryptographic erase | Use standard physical destruction methods |
| **USB Removable Media and Memory Cards** | Overwrite and verify | Not supported | Use standard physical destruction methods |
| **Embedded Flash Memory** | Reset to original factory settings | Not supported | Use standard physical destruction methods |
| **DRAM** | Not supported | Remove the DRAM from the device after switching off the power. | * Shred * Disintegrate * Pulverize |
| **EAPROM** | Not supported | Full chip purge as per OEM datasheet | * Shred * Disintegrate * Pulverize |
| **EEPROM** | Overwrite and verify | Not supported | Use standard physical destruction methods |
| **Optical Media** | Not supported | Not supported | * Shred * Disintegrate * Incinerate |

[2] Standard physical destruction methods include Shredding, Disintegration, Pulverization, Incineration

[3] DRAM - Dynamic Random Access Memory

[4] EAPROM - Electronically Alterable PROM

[5] EEPROM - Electronically Erasable PROM

**A) Clearing**

If comprehensive data removal from the media is not required, then non-specialist staff or contractors may carry out clearing. Typical clearing programs use sequential writes of patterned data, ensuring that data is not easily recovered using standard techniques and programs. To ensure that historical data is thoroughly removed it is advisable to make as many passes as is practicable.

**B) Purging**

Purging is a more advanced level of sanitization that renders media unreadable even through an advanced laboratory. After removal of media from its current security context there must be sufficient care taken to ensure that data is irretrievable. If purging of the media is required, a minimum of seven passes qualifies as a purging process.

**C) Destroying**

Destroying renders media unusable. Destruction techniques include but are not limited to disintegration, incineration, pulverizing, shredding and melting.

**Record of Data Destruction**  
Traceable and immutable records of data destruction are crucial to meet compliance by supplying the necessary audit trails. Therefore, the policy should include provisions for systematic recordkeeping of all the data destruction processes conducted in-house or by third-party vendors. Tamperproof certificates and reports of data destruction, maintained for individual storage media, can help businesses maintain the necessary documentation for compliance. NIST SP 800-88 recommends capturing the following details in the data destruction records:

* Manufacturer
* Model
* Serial Number
* Organizationally Assigned Media or Property Number (if applicable)
* Media Type (i.e., magnetic, flash memory, hybrid, etc.)
* Media Source (i.e., user or computer the media came from)
* Pre-Sanitization Confidentiality Categorization (optional)
* Sanitization Description (i.e., Clear, Purge, Destroy)
* Method Used (i.e., degauss, overwrite, block erase, crypto erase, etc.)
* Tool Used (including version)
* Verification Method (i.e., full, quick sampling, etc.)
* Post-Sanitization Confidentiality Categorization (optional)
* Post-Sanitization Destination (if known)
* For Both Sanitization and Verification:
  + *Name of Person*
  + *Position/Title of Person*
  + *Date*
  + *Location*
  + *Phone or Other Contact Information*
  + *Signature*
* Data backup details (optional)

Examples Report and Certificate

<https://www.bitraser.com/reports-and-certificates.php>

## **Additional Information - Tools**

Total Disk Wipe - All Platforms

• DBAN (Darik's Boot And Nuke) – an open-source boot disk utility that deletes the contents of any detected hard disks. (Note: This utility can also be used to delete specific files and folders.) • Physical destruction – Use a commercial solution such as Shred-it or remove the drive and hit it with a sledgehammer.

Selective File Wipe - Windows• Wipe File - Portable application that overwrites the specific disk space occupied by the file you'd like erased and leaves the rest of the disk untouched.

• DeleteOnClick - Integrates with the Windows shell, adding a "Securely Delete" option to the right click menu which engages a Department of Defense 5220.22-M over-write on the files.

• Eraser - In addition to securely deleting individual files, Eraser can be scheduled to perform regular overwrites of empty disc space ensuring you catch those orphan files hanging outside the reach of Windows.

• SDelete - Allows you to delete one or more files and/or directories, or to cleanse the free space on a logical disk (Microsoft/SysInternals). Runs on Windows XP and higher (clients) and Windows Server 2003 and higher.

Selective File Wipe - Mac OS X• Permanent Eraser - Although Mac users have had the "secure empty trash" option, based on a multiple pass DoD method, since OS 10.3, Permanent Eraser offers peace of mind for those needing more assurance

Selective File Wipe – Linux/Unix

• wipe – A unix command designed to securely erase files from magnetic media.

• shred – Linux/Unix file over-write/delete command.