**Cybersecurity Templates**

**Disposal & Destruction Procedure**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Disposal & Destruction Procedure** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** |  | **Effective Date:** |  |
| **Last Review Date:** |  | **Next Review Date:** |  |

Contents

[Disposal & Destruction Procedure 4](#_Toc207034121)

[1. Purpose 4](#_Toc207034122)

[2. Scope 4](#_Toc207034123)

[3. References 4](#_Toc207034124)

[4. Definitions (plain language) 4](#_Toc207034125)

[5. Roles & Responsibilities 5](#_Toc207034126)

[6. Triggers for Disposal 5](#_Toc207034127)

[7. End-to-End Procedure 5](#_Toc207034128)

[7.1 Initiation 5](#_Toc207034129)

[7.2 Pre-Sanitization Preparation 5](#_Toc207034130)

[7.3 Method Selection (Decision) 5](#_Toc207034131)

[7.4 Execution (Media‑Specific) 6](#_Toc207034132)

[7.5 Chain of Custody & Logistics 6](#_Toc207034133)

[7.6 Evidence & Documentation 6](#_Toc207034134)

[7.7 Completion & Review 6](#_Toc207034135)

[8. Metrics & Reporting 6](#_Toc207034136)

[9. Non-Compliance & Escalation 7](#_Toc207034137)

[10. Review & Maintenance 7](#_Toc207034138)

[11. Appendices 7](#_Toc207034139)

[Appendix A – Media Sanitization & Destruction Matrix (fill in per your tooling) 7](#_Toc207034140)

[Appendix B – Disposal Register (sample fields) 7](#_Toc207034141)

[Appendix C – Certificate of Destruction (minimum contents) 8](#_Toc207034142)

[Appendix D – Supplier Due Diligence Checklist 8](#_Toc207034143)

[Appendix E – RACI (example) 8](#_Toc207034144)

# Disposal & Destruction Procedure

# 1. Purpose

Define a standard, auditable method to sanitize, dispose of, and destroy information assets/media so that data cannot be recovered, while complying with legal, regulatory, and contractual obligations.

# 2. Scope

This procedure applies to all information assets and storage media (physical and virtual), end‑user devices, servers, network devices, removable media, optical media, backups, and MFDs/printers—owned or managed by [Organization], its subsidiaries, or third-party processors handling [Organization] data.

# 3. References

* [Organization] Information Security Policy, Data Retention Schedule, Incident Response Plan
* WEEE Regulations (as applicable) and local waste‑carrier licensing requirements
* NCSC guidance on secure sanitisation of storage media; device disposal practices
* ADISA / equivalent ITAD certification (where used)
* NIST Guidelines for Media Sanitization (informative)

# 4. Definitions (plain language)

**Sanitization:** Actions that irreversibly render data unrecoverable by reasonable means.  
**Clearing:** Logical techniques that protect against simple non-forensic recovery (e.g., factory reset).  
**Purging:** More robust logical techniques (e.g., cryptographic erase, full‑disk overwrite).  
**Destruction:** Physical rendering of media unusable (e.g., shredding, pulverization).

# 5. Roles & Responsibilities

* **Asset Owner:** Classifies the asset, initiates disposal request, approves method selection.
* **IT Operations (Custodian):** Executes sanitization/destruction; records evidence.
* **Information Security:** Approves methods, witnesses destruction (as required), and audits samples.
* **Legal/Privacy:** Confirms regulatory/contractual constraints (e.g., hold orders).
* **Vendor/ITAD:** Performs off-site/on-site services under contract; provides certificate of destruction (CoD).
* **Internal Audit/Compliance:** Reviews disposal register and evidence annually.

# 6. Triggers for Disposal

* Asset end‑of‑life, refresh, reassignment, warranty return (RMA), lease end, incident compromise, user off‑boarding, data migration.

# 7. End-to-End Procedure

## 7.1 Initiation

1. Submit a **Disposal Ticket** with: asset ID/serial, owner, location, data classification, media type, intended outcome (reuse, transfer, destruction), and requested completion date.
2. **Freeze** data processing on the asset; remove from general use; ensure backups are current and documented.

## 7.2 Pre-Sanitization Preparation

* Deregister device from asset and MDM inventories; revoke access tokens/keys; disable remote services.
* For mobiles/tablets: perform a factory reset and **remove SIM/memory cards** before hand‑off.
* For printers/MFDs: remove storage (if removable) and perform manufacturer reset; follow vendor guidance.

## 7.3 Method Selection (Decision)

Select **Clearing**, **Purging**, or **Destruction** based on:

* **Data classification** (highest rating governs),
* **Media type** (HDD, SSD, tape, optical, mobile, network appliance), and
* **Intended reuse** (reuse → sanitize; no reuse → destroy).  
  Note: If the media will not be reused, **destruction** is the default. Document the choice and approver.

## 7.4 Execution (Media‑Specific)

* **Magnetic HDD:** secure erase / full‑disk overwrite; degauss if appropriate; destroy if reuse not intended.
* **SSD/NVMe:** cryptographic erase (where supported) followed by physical destruction (shred/disintegrate) for high-risk data.
* **Tapes/Legacy Magnetic Media:** degauss then shred.
* **Optical (CD/DVD):** shred with rated equipment or use approved surface‑destroying devices; do not incinerate in-house.
* **Smartphones/Tablets:** factory reset; verify account sign‑out; remove SIM/memory; wipe via MDM if applicable.
* **Printers/MFDs:** remove/erase internal storage; factory reset; confirm address books/job logs cleared.
* **Network Devices/IoT:** follow vendor wipe and reset procedures; confirm config and logs are cleared (align with NCSC advice).

**Safety:** Do not drill or hammer drives; use certified destruction services. Incineration must never be performed in-house.

## 7.5 Chain of Custody & Logistics

* Use **approved mechanisms and vendors**; maintain custody from pickup to completion; log every hand‑off.
* For third parties: verify WEEE alignment, **waste‑carrier license**, and certifications (e.g., ADISA); retain CoD.

## 7.6 Evidence & Documentation

Record the following in the **Disposal Register** (Appendix B) and attach evidence: date/time, asset ID/serial, location, classification, method, tools used, operator, witness (if required), vendor details, **certificate ID**, and evidence storage path. Keep evidence per the defined retention period.

## 7.7 Completion & Review

* Security spot‑checks (sample of jobs/month).
* Close the ticket only after evidence is verified and inventory updated.
* Exceptions require risk acceptance, compensating controls, approver, and expiry date (tracked until closure).

# 8. Metrics & Reporting

* % of disposed assets with a complete evidence package
* % of vendor jobs with valid CoD
* Avg. days from initiation → completion
* of exceptions open > 30 days
* Quarterly sample audit pass rate

# 9. Non-Compliance & Escalation

Violations may trigger corrective actions and disciplinary measures per HR policy; material issues are escalated to [Risk & Compliance Committee].

# 10. Review & Maintenance

This procedure is reviewed **annually** or upon significant changes in technology, regulations, or supplier arrangements.

# 11. Appendices

## **Appendix A – Media Sanitization & Destruction Matrix (fill in per your tooling**)

|  |  |  |  |
| --- | --- | --- | --- |
| **Media Type** | **If Reused** | **If Not Reused** | **Notes** |
| HDD (magnetic) | Secure erase/complete overwrite; degauss for high risk | Shred/disintegrate | Degauss renders media unusable. |
| SSD/NVMe | Crypto erase + verify | Shred/disintegrate | SSDs typically require destruction. |
| Tape/Floppy | Degauss + verify | Shred |  |
| Optical (CD/DVD) | N/A | Shred/surface destroy | No in-house incineration. |
| Smartphones/Tablets | Factory reset; MDM wipe; remove SIM/memory | Shred if compromised |  |
| Printers/MFDs | Remove/erase storage; factory reset | Shred storage where removable |  |
| Network/IoT | Vendor wipe & reset | Destroy if risk dictates | Follow NCSC guidance. |

## Appendix B – Disposal Register (sample fields)

* Record ID, Asset ID/Serial, Asset Type/Model, Location, Owner, Data Classification, Method (Clear/Purge/Destroy), Tool/Service Used, Operator, Witness, Vendor, CoD ID, Evidence Path, Date/Time, Reviewer, Retention Until.

## Appendix C – Certificate of Destruction (minimum contents)

* Asset IDs/serials; method used; site/address; date/time; operator; witness; equipment used; batch ID; signature; vendor license/cert numbers (e.g., waste‑carrier).

## Appendix D – Supplier Due Diligence Checklist

* WEEE alignment; valid **waste‑carrier license**; applicable certifications (e.g., **ADISA**); insurance; facility security; chain‑of‑custody controls; sample CoD; right‑to‑audit.

## Appendix E – RACI (example)

* **Responsible:** IT Ops (execution), Vendor (off/onsite)
* **Accountable:** Information Security
* **Consulted:** Legal/Privacy, Asset Management
* **Informed:** Owner, Finance, Internal Audit