Table of Contents

[1. Introduction to Diposal and Destruction Policy 5](#_Toc77676426)

[2. Purpose 5](#_Toc77676427)

[3. Scope 5](#_Toc77676428)

[4. Policy 5](#_Toc77676429)

[**4.1 Disposal & Destruction of Paper based Records** 5](#_Toc77676430)

[**4.2 Disposal & Destruction of Media** 6](#_Toc77676431)

[**4.3 Destruction of Equipment** 6](#_Toc77676432)

[**4.4 Disposition of Excess Equipment** 6](#_Toc77676433)

[**4.5 Sending a hard drive out for repair or for data recovery** 6](#_Toc77676434)

[**4.6 Repairing a hard drive under warranty:** 7](#_Toc77676435)

[**4.7 Overwriting hard drives for sanitization** 7](#_Toc77676436)

[**4.8 Clearing data** 7](#_Toc77676437)

[**4.9 Reuse and redistribution of IT Asset** 7](#_Toc77676438)

[**4.10 Certification and Audit** 7](#_Toc77676439)

[**4.11 Record Asset Inventory** 7](#_Toc77676440)

[**4.12 Penalties** 8](#_Toc77676441)

**DOCUMENT REVISION CONTROL**

REVISION HISTORY

| **Date** | **Author** | **Version** | **Change Reference** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

REVIEWERS

| **Name** | **Position** | **Date** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

DISTRIBUTION

| **Date** | **Distributed to** | **Version** | **Distribution Format** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

APPROVALS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Approver** | **Title/Authority** | **Which specimen was destroyed** | **Signature** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

DESTRUCTION DETAILS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Record id** | **Description** | **Department** | **Destruction method** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**LIST OF ABBREVIATIONS**

|  |  |  |
| --- | --- | --- |
| **Index** | **Abbreviation** | **Stands For** |
| I | IT | Information Technology |
| 2 | SLA | Service Level Agreement |
| 3 | IOT | Internet of things |
| 4 | IAS | International Accounting Standards |
| 5 | FDP | Finance Department |
| 6 | ITSM | Information Technology Service Management |
| 7 | NDA | Non-Disclosure Agreement |

# Introduction to Diposal and Destruction Policy

IT Assets are very critical as they have information of sensitive data. <COMPANY NAME> is either creating, handling information and equipment’s, and it has responsibility to securely dispose of IT Assets, information & equipment, which are owned by <COMPANY NAME> and are no longer required or to be destructed for security reasons.

Disposal and Destruction Policy defines how the process of disposal and destruction of IT assets, namely information, Media and Equipment’s.

# Purpose

Disposal and Destruction policy defines the roles and responsibilities of staff in ensuring the secure disposal of <COMPANY NAME> IT Assets, Equipment & information. This policy aims to provide a rigorous method to ensure that IT Assets are deemed “End of Life” or for security reasons, must be disposed and destructed, as per the statute of this policy.

# Scope

The integrity of information assets must be always maintained.

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services with limited or unlimited access time.

All hardcopy that requires destruction are disposed and destructed using this policy guidelines.

External media shall be disposed of in a method that ensures that the confidentiality and security of Information Assets is not compromised.

# Policy

## **4.1 Disposal & Destruction of Paper based Records**

There are many records and documents shall be prepared & maintained in paper form. It is therefore essential that documents that are maintained on paper shall be shredded, or destroyed as per this policy, such that all information is disposed properly, per <COMPANY NAME> guidelines.

## **4.2 Disposal & Destruction of Media**

External or Internal Media, and information in the computers, servers et cetera form a part of Information Asset, media (CD-ROMs, DVDs, Disk, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data shall not be compromised.

The following steps must be adhered to:

1. Disposal & Destruction of Information Assets is the responsibility of each employee, employees will have to identify media which should be shredded and use this policy in its destruction.
2. External media should never be thrown in the trash, it should be destructed/destroyed.
3. When no longer needed all forms of external media are to be sent to the Information Security Department or appropriate personnel for proper disposal.
4. The media will be secured, and a log will be maintained, with authorized personnel / Information Security team until appropriate destruction methods are used.

## 

## **4.3 Destruction of Equipment**

Equipment Asset tags used for identifying equipment shall be removed before disposal and destruction of equipment.

Equipment to be destructed and disposed will erase all data, establish factory setting.

## **4.4 Disposition of Excess Equipment**

As the older computers and equipment are replaced with new systems, the older machines are held in inventory for various uses:

1. Old machines are regularly utilized for spare parts.
2. Old machines are used on an emergency replacement basis.
3. Old machines are used for testing new software.
4. Old machines are used as backups for other production equipment.
5. Old machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.

**4.5 Sending a hard drive out for repair or for data recovery:** The vendor repairing or recovering data on the hard drive must have signed an appropriate Business Associate Agreement with the Communication Disorders Clinic or Appalachian State University, stating that they will take proper care of the data. Once data is recovered or the hard drive is repaired the original hard drive must be returned to the owner so that the owner can dispose of it per this Communication Disorders Clinic policy for proper disposal of hard drives.

**4.6 Repairing a hard drive under warranty:**

1. In the special situation where a hard drive under warranty has failed and the manufacturer requires that the failed disk drive be returned, an appropriate Business Associate Agreement between the manufacturer and the Communication Disorders Clinic or Appalachian State University must be in place before the drive can be shipped to the manufacturer.
2. If the manufacturer will not sign a Business Associate Agreement, then the old drive must be properly destroyed, and the owner of the system must cover any costs associated with purchasing a new drive.

**4.7 Overwriting hard drives for sanitization:**

1. Overwriting is an approved method for sanitization of hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless information.
2. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented. Overwriting consists of recording data onto magnetic media by writing a pattern of fluxes or pole changes that represent binary codes.
3. Sanitization is not complete until the three overwrite passes and a verification pass are completed. A variety of software packages are available on the open market that properly performs this function.

**4.8 Clearing data:**

1. Clearing data such as formatting or deleting information removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data.
2. The clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing media intended for disposal outside of the Communication Disorders Clinic.

## **4.9 Reuse and redistribution of IT Asset**

Information Security Department shall undertake the necessary secure procedures to ensure any, and all sensitive data is removed, before IT Asset is redistributed.

## **4.10 Certification and Audit**

Successful deletion, disposal and destruction must be evidenced, and certification must be obtained and always recorded.

## **4.11 Record Asset Inventory**

Details of disposal, Destruction and deletion must be recorded and updated within the Information Security Inventory of asset database to ensure the <COMPANY NAME> has an up-to-date record of active IT assets and destroyed IT assets.

## **4.12 Penalties**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.