Policy number	Title:	Effective Date:
<your ID format>	ASSET & DATA SECURE DISPOSAL / RECYCLE PLAN	<your date format>

REFERENCES

- NIST CSF PR.AC-1, PR.DS-3, PR.IP-6

SUPPORTING DOCUMENTS

- **<This is a contents link space for any related documentation>**

CONTENTS

PURPOSE

Information systems capture, process, and store information using a wide variety of media, including paper. This information is not only located on the intended storage media but also on devices used to create, process, or transmit this information. These may require disposition to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality.

SCOPE

<company name> IT is responsible for all enterprise asset management functions. This secure disposal plan does not include assets that do not store, process, or transmit data, such as monitors and keyboards.

POLICY

<company name> must ensure that IT are made aware of this Asset Secure Disposal Plan to establish proper accountability for all data.

<company name> must ensure that confidential material is destroyed only by authorized and trained personnel, whether in-house or contracted, using methods outlined in this standard.

<company name> may use service providers for destruction purposes provided that the information remains secure until the destruction is completed. The service providers must follow this standard.

METHODS OF MEDIA SANITIZATION

The following table depicts the three types of sanitization methods and the impact of each method.

Sanitization Method	Appropriate Use	Description
Clear	If the media will be reused and will not be leaving **<company name>**'s control.	Protects confidentiality of information against an attack by replacing written data with random data.
Purge	If the media will be reused and leaving **<company name>**'s control.	Protects confidentiality of information against an attack through either degaussing or Secure Erase.
Destroy	If the media is to be retired and not be reused at all.	Intent is to destroy the media.

Method	Description
Clear	Use software or hardware products to overwrite user- addressable storage space on the media with data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all user- addressable locations. Overwriting cannot be used for media that is damaged or not rewriteable and may not address all areas of the device where sensitive data may be retained. The most common examples of 'Clear' would be the wiping and reusing of end user equipment These still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared data.
Purge	Some methods of purging include overwrite, block erase, and Cryptographic Erase, using dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands. Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing, and pulverizing. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending and Cutting. Degaussing renders a magnetic device purged Degaussing should never be solely relied upon for flash memory-based storage devices or for magnetic storage devices that also contain non-volatile non-magnetic storage. Degaussing renders many types of devices unusable (and in those cases, Degaussing is also a Destruction technique).
Destroy	There are many different types, techniques, and procedures for media destruction. While some techniques may render the data infeasible to retrieve, the device is not considered destroyed unless target data retrieval is infeasible using state of the art laboratory techniques. *Disintegrate, Shred, Pulverize, Melt, and Incinerate*. These sanitization methods are designed to destroy the media. They are typically carried out at an outsourced facility with

	the specific capabilities to perform these activities effectively, securely, and safely. The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the verification of Clear or Purge methods fails (for known or unknown reasons).

SANITIZATION DECISION PROCESS

The decision process is based on the reuse of the media type. **<company name>** IT will choose the type of sanitization to be used.

Disposal without sanitization should be considered only if information disclosure would have no impact on organizational mission.

SANITIZATION TIME FRAMES

Media should be sanitized by **<company name>** IT within 1 month of receiving. It should be considered a risk to leave data on systems for unnecessary lengths of time.

On occasion the sanitation process may be delayed pending legal, financial, or human resources related proceedings, in which case the media should be locked in a quarantine space until instruction is received to sanitize the data. IT should follow up at 6 monthly intervals if no instruction is received.

RE-USE AND RECYCLING OF IT EQUIPMENT

<company name> IT puts ‘reuse and recycle’ at the heart of IT service delivery, and many **<company name>** systems have several life-cycles as primary, secondary, and sometime tertiary functions before they are recycled. It is a cost-effective use of computing hardware, but to also reduces our carbon footprint and ensures hardware is only sent for recycle when every use has been covered. Furthermore, **<company name>** has purchased refurbished computer hardware for secondary roles to make the best use of hardware resources on the open market, and again, to minimise our carbon footprint and reduce our impact on the environment.

Whatever the use case, computer systems must be replaced before their end-of-service life to ensure that there is a constant level of support from the vendor for software updates, particularly security updates and patches.

IT HARDWARE LIFE-CYCLE

- **Data storage** - Primary storage systems have a lifetime for about four to five years after which they are repurposed into secondary storage systems such as engineering scratch data, development / staging storage for IT / DevOps development. Sometimes they will be used for longer-term data archive or data backup.

- **Networking** – Network infrastructure has up to a seven lifecycle before a replacement program is undertaken. Any networking equipment being replaced is often redeployed to engineering labs as switch capacity.
- **Desktops** – A typical **<company name>** desktop lasts about five to six years. During that time, they can have memory and storage upgrades to extend their practical life where applicable. Their 'second life' can often be found in software build nodes or engineering test harnesses for PCI development boards or test targets. When they get to about seven to eight years old, they are considered for recycle.
- **Laptops** – Laptops have a shorter life expectancy than desktops as they tend to get dropped, lost or broken. They are replaced after four to five years of use, and their 'second life' will be as redeployed as 'pool laptops', test laptops for Engineering.

RECYCLING

Once a computer or other IT equipment has come to the end of its life at **<company name>** it is sent for recycle. **<company name>** has a program of recycling with third party specialists who reuse where possible and ethically dispose of if not.

No computer leaves **<company name>**'s ownership until the asset has been sufficiently accounted for. **<company name>** IT will organise the recycling of computer systems. This is performed periodically and any reimbursement, after recycling costs have been accounted for, is given to charities.

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY