



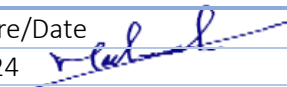
# Secure Asset Disposal Process


Doc. Control Number	Version
SNL-67	0.2



## Document Reference

Item	Description
Title	Secure Asset Disposal Process
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	5 March 2025
Revision-Date	5 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/3/2024 

## Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	5 March 2024	Muhaned Ali	First Release
0.2	11 Aug 2024	Muhaned Ali	The document has been reviewed



## Contents

1. Secure Asset Disposal Process .....	4
--	---

## 1. Secure Asset Disposal Process

### 1.1 Asset Identification

- a) At the end of their lifecycle or when deemed obsolete, it is the responsibility of the business owner or IT team to identify assets such as hard drives, USB drives, and physical documents for disposal.

### 1.2 Asset Classification

- a) Assets are classified based on sensitivity levels: public, internal use only, restricted, or confidential.

### 1.3 Data Destruction Plan

- a) Public data: Secure erase using certified software. (KillDisk-Software)
- b) Internal Use Only data: Secure erase followed by physical destruction (drilling).
- c) Restricted data: Physical destruction through shredding or degaussing.
- d) Confidential data: Combination of secure erase, shredding, and degaussing.

### 1.4 Secure Storage

- a) Assets awaiting disposal are stored in a designated, locked area accessible only to authorized personnel.

### 1.5 Secure Erase

- a) For digital assets, use secure erase techniques that follow industry standards, such as NIST Special Publication 800-88, to effectively erase data and make it unrecoverable.

### 1.6 Physical Destruction

Physical destruction methods are employed for hardware and physical documents:

- a) Hard drives and other storage media are drilled through or shredded using industrial-grade shredders.
- b) Physical documents are shredded using cross-cut shredders or pulped to render them unreadable.

### 1.7 Roles and responsibility

- a) The IT team is responsible for asset disposal and should attend each disposal process, documenting it accordingly.

### 1.8 Documentation

- a) Detailed records are maintained for each asset disposal, including asset identification, disposal method, and personnel involved. A certificate of destruction is issued for third-party disposal services.

### 1.9 Third-Party Disposal

- a) If outsourcing disposal, third-party vendors must comply with strict security protocols and provide certification of secure disposal.

### 1.10 Verification

- a) The IT team must verify that destruction is conducted to ensure all assets have been effectively destroyed. This may involve physical inspection or auditing of digital data erasure logs.

### 1.11 Compliance Review

- a) The GRC Team must conduct regular reviews of the Secure Asset Disposal Process to ensure compliance with industry standards, regulatory requirements, and technological advancements.