




Secure Asset Disposal Policy

Doc. Control Number	Version
SNL-43	0.3



Document Reference

Item	Description
Title	Secure Asset Disposal Policy
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	21 July 2024
Revision-Date	21 July 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	7/21/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	7/21/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	7/21/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	23 May 2023	Muhaned Ali	First Release
0.2	19 July 2023	Muhaned Ali	The policy has been revised and updated.
0.3	21 July 2024	Muhaned Ali	The policy has been reviewed



Contents

1. Overview	4
2. Policy Guidelines	4
3. Compliance and Enforcement.....	5

1. Overview

This Procedure establishes guidelines for the secure disposal of information assets within SNLC. This is to ensure that assets are disposed of in a secure manner based on their classification and labelling, as defined in the Asset Inventory. Secure disposal practices are implemented to prevent unauthorized access, disclosure, or recovery of sensitive information during the disposal process.

2. Policy Guidelines

2.1 Asset Disposal Classification

- a) All information assets within SNLC shall be classified based on their sensitivity, criticality, and regulatory requirements, as defined in the Asset Inventory.
- b) Asset disposal rules shall be established for each classification level, outlining the appropriate disposal methods and procedures.

2.2 Disposal Methods

- a) Non-Confidential Assets
 - Non-confidential assets, including publicly available or non-sensitive information, may be disposed of through regular waste management processes in compliance with local regulations.
- b) Confidential and Highly Confidential Assets
 - Confidential and highly confidential assets shall be disposed of using secure methods that ensure data cannot be easily recovered.
 - Secure disposal methods may include physical destruction (e.g., shredding, incineration) or secure digital data erasure techniques approved by the organization.

2.3 Secure Erase for Digital Assets

- 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.
- b) Utilize software tools (KillDisk-Software) or hardware devices specifically designed for secure data erasure.

2.4 Physical Destruction for Physical Assets

- a) For physical assets, such as hard drives, tapes, or other storage media, employ physical destruction methods to render the information irrecoverable.
- b) Options include drilling through the storage media or using specialized shredding equipment.

2.5 Disposal Procedures

- a) Asset owners or designated personnel shall be responsible for initiating and overseeing the disposal process.
- b) Disposal procedures shall be documented and include the following steps:
 - Asset identification and verification of classification and labeling.
 - Selection of the appropriate disposal method based on the asset's classification.
 - Execution of the disposal method in a secure and controlled environment.
 - Documentation of the disposal process, including date, method used, and personnel involved.
 - Approval and sign-off by the asset owner or designated personnel
- c) Review & Revoke Access form must be maintained mandatorily for all assets used to process or store Saudi Aramco data and information to sanitize the end of the Data Life Cycle, or by the of the retention period as stated in the contract, if defined.

This includes all data copies such as backup copies created at any sites of SNLC company. SNLC shall certify in writing to Saudi Aramco that the data sanitization has been completed.

2.6 Disposal Auditing and Records

- a) Regular audits shall be conducted to ensure compliance with the asset disposal policy and procedures.
- b) Disposal records, including disposal logs, certificates of destruction, or any relevant documentation, shall be maintained for a specified period as per organizational and regulatory requirements.

3. Compliance and Enforcement

3.1 Non-compliance with this policy may result in disciplinary action, including but not limited to retraining, suspension, termination, and legal consequences, as appropriate.

3.2 Policy Review

- a) This policy will be reviewed on a periodic basis to ensure its continued relevance and effectiveness. Any updates or modifications to this policy shall be communicated to all relevant employees and stakeholders.