Data Sanitization Policy

Doc. Control Number	Version
SNL-60	0.2

Document Reference

Item	Description
Title	Data Sanitization Policy
Department	Cybersecurity department
Version No	1.0
Status	Draft
Type	DOCX
Publish-Date	22 August 2023
Revision-Date	22 August 2024

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	22/8/2023

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	23/8/2023

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	23/8/2023

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	Aug 2023	Muhaned Ali	First Release
0.2	11 Aug 2024	Muhaned Ali	The policy has been reviewed

Contents

1. Overview

The data sanitization policy provides a process of irreversibly removing or destroying data stored on a memory device or in hard copy form. It is important to use the proper technique to ensure that all data is purged.

2. Purpose

The purpose of this policy is to empower all applicable entities with a clear list of acceptable methods, options, and corresponding instructions to produce consistent reliable results when Data Sanitization is required. Approved Sanitization methods are listed where available and only apply to the assigned media type in the Process Requirements section. The sanitization procedure selected should be the option that best suits the operational needs.

3. Scope

All employees of SNLC have a responsibility to ensure the confidentiality of SNLC information residing on the computer systems and other digital storage devices as well as any non-reusable media they use, whether it be SNLC or personally owned. All computers and digital storage devices including, but not limited to desktop workstation, laptop, server, notebook, tablet, and handheld computer hard drives; external hard drives; and all external data storage devices such as disks, flash drives, DVD, and CD, are covered under the provisions of this policy.

4. Policy

4.1 Non-Sensitive Data

a) SNLC data other than Sensitive data may be deleted and/or reformatted.

4.2 Sensitive Data

a) Sensitive Data must be sanitized or disposed of in a manner that leaves such Data fully unrecoverable.

b) SNLC must implement a sanitization process before any assets are loaned, donated, destroyed, transferred, or surpluses. The process must be aligned to industry best practices, such as NIST 800-88.

4.3 Device Transfer within SNLC

a) If the original system owner and the new recipient have the same rights to view the High-Risk Data stored on the device, there is no need for data sanitization. If the new recipient has no business justification to access the stored High-Risk Data, the files containing this data must be sanitized according to the Data Sanitization Guidelines below. The device may be transferred without removing any Moderate or Low Risk Data.

4.4 Device Transfer Between Organizations

a) All High-Risk Data stored on the device must be sanitized unless an exception is approved and documented in advance by organization management. In addition, all Moderate Risk Data stored on the device must be sanitized according to the Data Sanitization Guidelines below.

b) Assets used to process or store Saudi Aramco data and information must be sanitized by the end of the Data Life Cycle, or by the end of the retention period as stated in the Contract, if defined. This includes all data copies such as backup copies created at any Third-Party site(s). Third Party shall certify in writing to Saudi Aramco that the data sanitization has been completed.

4.5 Device Disposal or Device Transfer off SNLC

a) If a device is to be disposed of or transferred to a party outside of SNLC, the SNLC InfoSec team must sanitize or remove all device storage regardless of if the device is known to contain any High, Moderate, or Low Risk Data. Also, the local property administrators should be prepared to either sanitize or destroy the disk themselves according to the Data Sanitization Guidelines below (and keep a record of the activity) or contact the Information Security Office for assistance.

4.6 Personally Owned Devices Leaving SNLC

a) All High, Moderate, or Low Risk Data stored on the device must be sanitized according to the Data Sanitization Guidelines below unless an exception is approved and documented in advance by organization management.

4.7 Sanitization Methods

Method	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the The overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is suitable.
Purge	Degaussing and executing the firmware Secure Erase command are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field to disrupt the recorded. magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.
Destroy	There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack. • Disintegration, Pulverization, Melting, and Incineration. These sanitization methods are designed to destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • Shredding. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding, or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm2).

5. Data Sanitization Guidelines

5.1 Hard Drive and Removable drives

ATA Solid State Drives (SSDs) (including PATA, SATA, eSATA, and SCSI)	▪ Ensure that TRIM is enabled on the drive and in the operating system, then delete all files and folders: - **Mac OS X** - **Windows:** Open a command prompt and run the following command: “fustily behaviour query disabledeletenotify” - “DisableDeleteNotify = 0” means that Windows TRIM commands are enabled. - “DisableDeleteNotify = 1” means that Windows TRIM commands are disabled. To enable, run: "fsutil behavior set disabledeletenotify 0”. - To wiping the data, you will use KillDisk software
USB Removable Media and Memory Cards	- Overwrite the full drive/card with at least two write passes to include a pattern in the first pass and its complement in the second pass. Verify that the data was overwritten. - To wiping the data, you will use KillDisk software. and/or. - Physically shred the drive such that the resulting particles have a maximum edge length of 2 mm and a maximum surface area of 4 mm2.
CD, DVD, Blu-ray Disc	- Physically shred the optical media such that the resulting particles have a maximum edge length of 0.5 mm and a maximum surface area of 0.25 mm2. and/or. - Incinerate the optical media (i.e., reduce to ash) using a licensed facility.

5.2 Hard Copy Storage

Paper	- Shred paper documents using a crosscut shredder that produces particles no larger than 1 mm x 5 mm. or - Pulverize/disintegrate paper documents using a disintegrator device equipped with a 2.4 mm (or smaller) security screen.

6. Policy Compliance

6.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

6.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

6.3 Non-Compliance

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