Information Deletion Procedure

HT-ISMS-SOP-38

Document Control

Document Title	Information Deletion Procedure		
Document ID	HT-ISMS-SOP-38		
Document Type	Procedure	Classification	Internal
Version	1.0	Release Date	
Author	Name		
	Designation		
Reviewer	Name		
	Designation		
Approver	Name		
	Designation		

Revision History		
Version	Revision Description	Release Date
1.0	Initial Release	

Document Distribution			
Name	Department	Designation	Company
	IT	System Admin	HackTech
	IT	Information Security	HackTech

Table of Contents

1. Purpose

The purpose of this document is to define the procedures for securely deleting information within the organization.

2. Scope

This procedure applies to all employees, contractors, and third parties who handle or manage organizational information, whether physical or digital.

3. Roles and Responsibilities

Data Owner: Responsible for ensuring the proper deletion of their managed data in accordance with this procedure.

4. Information Deletion Methods

4.1 Physical Data Deletion

- **Paper Documents**
    - Confidential physical documents are shredded using shredders such as to prevent unauthorized access or data reconstruction.

5. Secure Disposal Procedures

5.1 Digital Devices

Before decommissioning or reallocating devices such as laptops and desktops we perform formatting devices ensuring all sensitive information is deleted.

6. Deletion of Personally Identifiable Information (PII)

In HackTech, we treat PII such as Aadhaar card numbers, PAN card numbers, passport numbers, and financial information with utmost care. This data is deleted in compliance with ISO27001 using secure deletion process. Customer and employee data is securely deleted once retention periods have expired or it is no longer needed for business purposes.

7. Monitoring and Verification

Audits are conducted each month to check if the process related to information deletion is duly followed or not.
Additionally, evidence is checked, wherever it is possible to be checked.

8. Third-Party Data Deletion

For data shared with third-party vendors or cloud service providers, we ensure their data deletion processes meet HackTech’s deletion policy. Also, we take written confirmation from vendors to verify that data has been securely deleted.

9. Exceptions

If any exceptions to this information deletion procedure are required, they must be documented in Jira and approved by the IT Manager and the Compliance Team. Exceptions are reviewed regularly to ensure their continued validity.