# Data Leakage Prevention Procedure

## HT-ISMS-SOP-33

# Document Control

| | | | |
|---|---|---|---|
| Document Title | Data Leakage Prevention Procedure | | |
| Document ID | HT-ISMS-SOP-33 | | |
| 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. Introduction

Data is a vital asset to our company, and its protection is essential to our operational success, customer trust, and compliance with legal and regulatory requirements

# 2. Objective

The objective of this procedure is to:

- Prevent data breaches and unauthorized data disclosures.

# 3. Scope

This procedure applies to all employees, contractors, and third-party users who handle sensitive data within the company. It covers all types of data, including electronic, printed, and verbal information.

# 4. Roles and Responsibilities

## 4.1 IT Department

- Implement and maintain DLP tools and technologies.

## 4.2 Employees

- Follow DLP policies and procedures.

## 4.3 Security Team

- Handle data breach incidents according to the incident response plan.

# 5.Data Leakage Prevention Control

## 5.1 Web DLP

To prevent Data Leakage, HackTech has DLP in place for systems and services, HackTech follows the below guidelines for a DLP Solution

### Configuration

- IT Team configured Quick Heal Seqrite web DLP policies to filter web traffic for sensitive data based on predefined rules as well as custom rules.

### Monitoring

- Security Team Monitor real-time web traffic using Quick Heal Seqrite DLP dashboard.
- Security Team Review and analyze alerts generated by the DLP system to detect potential policy violations or security incidents.

### Incident Response

- Security Team Investigate and assess alerts triggered by Quick Heal Seqrite DLP to determine the nature and severity of incidents.

## 5.2 Email DLP

### Configuration

- IT Team configured Quick Heal Seqrite email DLP policies to enforce encryption, content filtering, and data leakage prevention rules as well as custom rules.

### Policy Enforcement

- DLP enforce policies that restrict the transmission of sensitive data outside the organization or to unauthorized recipients.

### Monitoring and Alerts

- Security Team monitor email traffic using Quick Heal Seqrite DLP dashboard.

### Incident Handling

- Security Team Investigate incidents identified by Quick Heal Seqrite DLP alerts to determine root causes and impacts.