Configuration Management Procedure

HT-ISMS-PL-35

Document Control

Document Title	Configuration Management Procedure		
Document ID	HT-ISMS-SOP-35		
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

Configuration management is essential for ensuring the integrity, security, and compliance of our organization's IT infrastructure. This procedure outlines the processes involved in defining, managing, and monitoring configurations to support operational efficiency and safeguard sensitive information.

2. Purpose

The purpose of this configuration management procedure is to provide a structured approach to managing IT configurations. This ensures all changes are systematically controlled, tracked, and monitored to minimize unauthorized changes, maintain compliance with regulatory standards, and enhance system reliability and security.

3. Scope

This procedure applies to all IT assets, including hardware, software, network components, and configurations within our organization. It covers the processes involved in defining, managing, and monitoring configurations to ensure they meet business requirements and compliance standards.

4. Configuration Management Process

1. Define Configuration

Defining configuration involves identifying and documenting the configuration items (CIs) that need to be managed. This includes:

I. Network Configuration:

- The network is secured with the Sophos authentication client.

- Network access is restricted, and authentication credentials are provided by the IT team at the time of onboarding through a Jira ticket.

II. Asset and Server Configuration:

- When providing new assets to users, the IT team formats the devices and installs necessary and authorized software based on role-specific requirements.

2. Manage Configuration

Managing configuration involves maintaining and updating documented configurations to ensure consistency and compliance:

I. Change Management:

- Any changes to configurations must be documented and approved through a Jira ticketing system.

II. Configuration Backup and Recovery:

- Regular backups of configurations are taken to ensure data integrity and enable quick recovery in case of failures or breaches.

III. Documentation:

- All configuration management activities, including changes, approvals, and installations, are thoroughly documented.

3. Monitor Compliance

Monitoring compliance involves continuously overseeing the configurations to ensure they adhere to established policies and standards:

I. **Network Monitoring:**

- The security team monitors the network using the Sophos dashboard to detect and respond to intrusions, DDoS attacks, or any other suspicious activities.

II. **Asset Monitoring:**

- ManageEngine is used to monitor all assets and servers, tracking hardware and software usage.

III. **Incident Response Management:**

- Logs and management activities are maintained for troubleshooting and incident response.

5. Conclusion

Effective configuration management is essential for maintaining the integrity, security, and compliance of our IT infrastructure. By defining, managing, and monitoring configurations, we ensure that all IT assets are correctly identified, controlled, and safeguarded against unauthorized changes and potential security threats. This structured approach supports our organization’s commitment to operational excellence and regulatory compliance.