Configuration Management Policy

HT-ISMS-PL-21

Author- Saurav Chaudhari

CONFIDENTIALITY

This document is prepared by HackTech**.** All rights are reserved. No part of this document may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying without the written permission of HackTech. If this copy of the document is a hard copy, it is likely to be an obsolete version. Please check with the author of this document, to ensure that you are referring to the current version.

Document Control

Document Title	Configuration Management Policy		
Document ID	HT-ISMS-PL-21		
Document Type	Policy	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
	Operations	VP Projects	HackTech

Author- Saurav Chaudhari

Table of Contents

Author- Saurav Chaudhari

1. Introduction

HackTech uses a wide variety of components in creating and running its ICT infrastructure and end-user devices. These consist of hardware, software, cloud services, and networks, all of which are potentially vulnerable to attacks from various sources. To mitigate the risk of these components becoming compromised, it is important to identify the most appropriate ways of configuring them and ensure these methods are consistently applied across our ICT landscape.

2. Purpose

The purpose of this policy is to define the principles and rules for configuring the hardware, software, cloud services, and networks that makeup HackTech ICT environment.

3. Scope

This policy applies to all systems, people, and processes that constitute the organization's information systems, including board members, directors, employees, suppliers, and other third parties who have access to HackTech systems.

4. Configuration Management Policy

4.1 Security Settings for New Components

New components that make up HackTech hardware, software, services, and networks must have their required security settings defined and correctly configured prior to their implementation within our ICT environment.

4.2 Periodic Review of Existing Components

Configurations of existing components must be reviewed periodically to ensure they meet the requirements of this policy. These components include, but are not limited to:

- Endpoint devices, such as desktops, laptops, mobile phones, and tablets

4.3 Standard Templates and Documentation

Where possible, standard templates will be used to document the required configuration of ICT components. These templates will be subject to change and version control.

4.4 Information Sources for Configuration Standards

The configurations defined will take appropriate account of available sources of information about securing the relevant components, such as vendor templates, guidance from

Author- Saurav Chaudhari

cybersecurity authorities, best practice organizations, system hardening guides, and our own information security policies.

4.5 Protection of Configuration Details

Details of configuration standards will be protected as sensitive information which would be of use to an attacker.

4.6 Regular Review and Updates

Configuration standards is been reviewed on a regular basis and kept up to date with changes in the components (such as new hardware or software versions) and the threats and vulnerabilities they face.

4.7 Monitoring and Correction of Deviations

The correct configuration of components will be monitored, and instances where existing settings deviate from the established standard will be investigated and, if necessary, corrected.

5. Conclusion

By adhering to this configuration management policy, HackTech aims to ensure the security and integrity of its ICT components, mitigate risks associated with misconfigurations, and maintain compliance with legal and regulatory requirements. This proactive approach helps safeguard our information systems and assets, ensuring the continued trust of our stakeholders.

By following this structured and comprehensive configuration management policy, HackTech can effectively manage the security and integrity of its ICT environment, maintaining a robust defense against potential threats and vulnerabilities.

Author-Saurav Chaudhari