Langslide

Configuration Management Policy

Version 1.0

PURPOSE

This Configuration Management Policy aims to ensure the consistent management of configuration items (CI) across Rudramsa Systems Pvt. Ltd. (herein referred to as Organization) and maintain the integrity, confidentiality, and availability of our information assets.

SCOPE

This policy applies to all employees, contractors, and third-party service providers who can access or handle the ISMS or its components. The policy covers all configuration items critical to the ISMS, including hardware, software, network devices, and other organizational elements.

DEFINITION

- **ISMS:** Information Security Management System
- **Configuration Item:** A configuration item (CI) is any service component, infrastructure element, or other item that needs to be managed to ensure the successful delivery of services.

RESPONSIBILITIES

- The Chief Information Security Officer (CISO) oversees the Configuration Management process and ensures that it is consistent with the organization's overall Information Security Management System (ISMS).
- The IT and DevOps Head are responsible for implementing the configuration management process.
- All employees, contractors, and third-party service providers are responsible for following the Configuration Management process and ensuring that all configuration items are recorded and stored securely.

POLICY

Configuration Management Objectives

The objectives of Configuration Management are to:

- Identify all configuration items that require management and control.
- Define the structure and documentation requirements for configuration items.
- Establish a process for controlling configuration items' creation, modification, and deletion.
- Ensure that all configuration items are recorded and stored securely.
- Maintain accurate and up-to-date information on the status and location of all configuration items.

Identification of Configuration Items (CI)

- All information assets, including hardware, software, and documentation, must be identified as configuration items (CI).
- The Configuration Item identification process must ensure that all assets are uniquely identifiable and consistently labeled, tracked, and controlled throughout their lifecycle.
- IT teams shall manage an up-to-date configuration of systems in the CMDB.

Baseline Configuration

- A baseline configuration must be established for all CIs, defining the agreed-upon configuration settings, versions, and other attributes.
- Any changes to the baseline configuration must be managed, documented, and approved by authorized personnel.

Change Management

- All changes to Configuration Items must be recorded, authorized, tested, and approved before implementation.
- The change management process must ensure that changes are made in a controlled and consistent manner and that any impact on the security, functionality, and performance of the information assets is evaluated and managed.

Configuration Control

- Configuration control must be maintained throughout the lifecycle of Configuration Items, including acquisition, development, testing, deployment, and disposal.
- The configuration control process must ensure that changes to Configuration Items are managed and documented and that unauthorized changes are identified and remediated.

Configuration Verification and Audit

- The configuration management must be regularly verified and audited to ensure compliance with this policy and regulatory requirements.
- Any deviations or non-compliance must be documented and reported to the appropriate management level for remediation.

Retention and Disposal of Configuration Items

- Configuration Items must be retained and disposed of by regulatory requirements and organizational policies.

- Any disposal of Configuration Items must be secure and controlled, ensuring that any residual information is effectively destroyed or made unreadable.

Training and Awareness

Training

- All personnel with access to information assets must be trained on the configuration management processes and procedures and their roles and responsibilities.

Awareness

- All personnel must be aware of the importance of configuration management in ensuring the security, functionality, and performance of the organization's information assets.

Monitoring and Review

Monitoring:

- The configuration management process must be monitored regularly to ensure compliance with this policy and regulatory requirements. This includes monitoring changes to CIs, identifying unauthorized changes, and monitoring compliance with the configuration control process.

Review:

- The configuration management policy and processes must be reviewed regularly or when significant changes occur to the information assets or organizational structure. The review must evaluate the effectiveness and efficiency of the configuration management processes and identify improvement opportunities.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Mar 14 2026	Initial Release	Pronoy	Kartikeya	Kartikeya