Family Law Software
A CENTERBASE COMPANY

Configuration Management Plan (CMP)

This document outlines the organization's plan for identifying, managing, monitoring, and enforcing secure configurations across all information systems throughout their lifecycle.

1. Scope and Policy

This plan applies to all **Configuration Items (CIs)** within the organization's environment, including hardware, software, operating systems, network devices, and application configurations, from development through decommissioning.

Goal: To ensure that only authorized and tested configurations are deployed and maintained, minimizing security risks and operational drift.

2. Configuration Item (CI) Identification and Management

2.1. Identification and Inventory

The organization has **established processes for identifying and managing configuration items throughout the system development life cycle (SDLC)**:

1. **Initial Identification:** During the **Design and Development** phase of the SDLC, every new system component is identified and registered as a CI in the centralized Configuration Management Database (CMDB).
2. **Baseline Definition:** A secure, approved configuration baseline is defined for each CI type (e.g., Windows Server 2022 Baseline, Cisco Router Baseline) according to the Infrastructure Hardening Policy.
3. **Lifecycle Tracking:** The CMDB tracks the CI's status (e.g., *In Development, Testing, Production, Decommissioned*) and links it to its approved configuration baseline and corresponding change history (RFCs).

2.2. Configuration Change Control

All modifications to a CI's approved configuration must follow the **Change Management Process**. No configuration change is permitted without formal review, authorization, and successful testing.

3. Configuration Enforcement and Monitoring

3.1. Enforcing Defined Configurations

Plans are used to enforce defined configurations for newly installed systems as well as for operational systems:

1. **New Installations (Deployment):** All new systems are deployed using secure, pre-configured images or automated build scripts (e.g., Infrastructure as Code, Group Policy Objects) that install the approved CI baseline configuration automatically.
2. **Operational Systems (Drift Prevention): System management tools** (e.g., Configuration Management Automation platforms, centralized policy enforcement tools) are used to continuously compare the current state of operational CIs against their approved baseline. Any deviation (configuration drift) is logged and automatically remediated or flagged for immediate investigation.

3.2. Monitoring and Auditing

System management tools are used to monitor configurations to ensure compliance and detect unauthorized changes:

1. **Continuous Monitoring:** Configuration Management tools are scheduled to perform daily scans against critical CIs to check for compliance with the security baseline.
2. **Alerting:** Alerts are generated when configuration drift is detected, prioritized by the severity of the deviation (e.g., an unauthorized service installed vs. a minor file permission change).
3. **Auditing:** Configuration compliance reports are generated monthly and reviewed by the Security and IT Operations teams to identify recurring non-compliance issues and adjust baselines or enforcement mechanisms as necessary.

4. Automatic Logoff (Time-Out Facilities)

The plan establishes rules for invoking time-out facilities that automatically log off computing devices to protect systems from unauthorized access when unattended.

Device Type	**Condition**	**Time-Out Period**	**Action**
Servers (Administrative Access)	Administrative Console or Remote Session (e.g., RDP, SSH)	**15 Minutes** of inactivity	Automatically disconnect session and lock the console.
Workstations/Laptops	Endpoint Console (User Session)	**10 Minutes** of inactivity	Automatically activate a password-protected screen saver.
Network Devices	Console/CLI Access	**5 Minutes** of inactivity	Automatically log off the user session.

These time-out facilities are enforced globally via central policy management tools (e.g., Group Policy, centralized configuration templates) and cannot be overridden by local users.