Family Law Software
A CENTERBASE COMPANY

Patch Management Policy and Process

This document outlines the organization's policy and process for managing, testing, and applying security and functional patches to systems, network infrastructure, and applications. The objective is to maintain security integrity, system performance, and compliance by promptly mitigating vulnerabilities.

1. Policy Review and Governance

- **Annual Review:** This Patch Management Policy document and the associated processes are **reviewed and approved by management at least annually** (or upon significant infrastructure/regulatory changes) to ensure continued effectiveness and alignment with the current threat landscape and organizational needs.
- **Notifications:** The organization maintains subscriptions and configurations to enable **automated notifications** for official vendor updates regarding system and third-party application patches. This ensures immediate awareness when patches are available.

2. Patch Management Lifecycle and Implementation Cycle

The organization maintains a structured cycle for patch implementation across all assets:

2.1. Discovery and Categorization

1. **Vulnerability Scanning:** Continuous monitoring and scheduled scans identify missing patches across the environment (servers, endpoints, network devices, and applications).
2. **Patch Categorization:** Patches are categorized based on the vendor-assigned severity level and the internal impact assessment.

2.2. Criticality Timescales for Implementation

The organization has **defined a cycle of implementing patches** based on the following criticality timescales, which dictate the maximum allowable time from patch availability/discovery to successful deployment in the production environment:

Criticality Level	Risk Description	Remediation Timescale (Maximum)
Critical	Exploitable vulnerability with a high severity score, active exploitation, or poses an imminent threat to business continuity or sensitive data.	**7 Calendar Days**
High	Significant vulnerability that could lead to unauthorized access or system compromise, but is not currently under active exploitation.	**14 Calendar Days**
Medium	Moderate vulnerability, typically requires local access or user interaction to exploit, or affects a non-critical system.	**30 Calendar Days**
Low/Informational	Minor vulnerabilities, configuration updates, or non-security-related functional patches.	**Scheduled with next standard maintenance window (up to 60 days).**

2.3. Testing of Security Patches

Testing of security patches occurs prior to deployment to the production environment to prevent operational disruption, configuration errors, or unexpected system outages.

1. **Test Environment:** Patches are first deployed to a designated, non-production test environment (e.g., Staging/UAT) that accurately mirrors the production system.
2. **Test Procedures:** Key business processes, application functionality, and security controls are validated post-patch installation.
3. **Approval:** Successful testing is documented and provides the necessary authorization to proceed with production deployment.

2.4. Deployment and Verification

1. **Deployment:** Patches are deployed following the **Change Management Process** and the defined remediation timescales. Deployments for non-critical patches typically occur during scheduled maintenance windows.

2. **Verification:** Post-deployment checks ensure the patch was successfully applied and systems are operating normally.

2.5. Monitoring and Reporting (End-User Devices)

- **Monitoring Success:** Centralized patch management tools (e.g., MDM/Endpoint Management Systems) are used to **monitor end-user devices** (laptops, desktops, mobile devices) to ensure that security patches have been **applied successfully**.

- **Compliance Reporting:** Systems that fail to patch successfully or fall out of compliance within the defined timescale are automatically flagged, isolated (if necessary), and subjected to mandatory remediation by IT support.