Wyoming Judicial Branch

Patch Management Policy

Policy Approver(s)	Wyoming Judicial Council
Effective Date	June 10, 2024
Review Period	Annually

I. PURPOSE

The purpose of this policy is to outline the processes and responsibilities necessary to ensure the effective and secure management of software and hardware patches within Wyoming Judicial Branch (WJB). This policy aims to protect the Branch's information technology systems from known vulnerabilities, enhance system performance, and align with industry best practices.

II. DEFINITIONS

A. "Patch Management" means the process of identifying, acquiring, installing, and verifying patches for software and systems. Patches are typically small updates released by software vendors to address specific issues such as security vulnerabilities, bugs, or minor feature enhancements. The primary focus of patch management is to keep software secure and functioning efficiently without altering its core functionality. It's a routine, ongoing process aimed at maintaining operational stability and security compliance.

B. "Information Technology Systems" means the combination of hardware, software, and networks that are used to store, retrieve, transmit, and manipulate data.

III. APPLICATION

This policy applies to all justices, judges, employees, and contractors of the WJB involved in the management, operation, and use of information technology systems.

IV. INFORMATION STATEMENT

The WJB commits to regularly updating and patching all software and systems to protect against vulnerabilities and threats. This includes operating systems, applications, and security software across all platforms and devices.

V. RESPONSIBILITIES

A. Information Technology Division: Coordinates the patch management process, including identification, testing, deployment, and verification of patches.

B. Justices, judges, employees, and contractors of the WJB: Comply with all notifications and instructions related to patch management activities.

VI. PATCH MANAGEMENT PROCESS

Patch management must be prioritized based on the severity of the vulnerability the patch addresses. In most cases, severity ratings are based on the Common Vulnerability Scoring System (CVSS). A CVSS score of 7-10 is considered a high impact vulnerability, a CVSS score of 4-6.9 is considered a moderate impact vulnerability and a CVSS of 0-3.9 is considered a low impact vulnerability.

A. Identification: Regularly review available patches from vendors and security advisories.

B. Assessment: Evaluate patches for relevance, criticality, and potential impact.

C. Testing: Test patches in a non-production environment to ensure compatibility and non-disruption.

D. Communication: Communicate promptly and clearly via GovDelivery or directly as needed if a patch is assessed to have substantial impact on end users.

E. Implementation: Schedule and deploy patches in a manner minimizing operational impact.

F. Verification: Confirm successful patch deployment and system functionality.

To the extent possible, the patching process will follow the timeline contained in the table below:

Impact/Severity	Patch Initiated	Patch Completed
High	Within **24 hours** of patch release	Within **1 week** of patch release
Medium	Within **1 week** of patch release	Within **1 month** of patch release
Low	Within **1 month** of patch release	Within **2 months** of patch release

VII. PATCH MANAGEMENT SCHEDULE

A. Workstations – Tuesdays, 1:00 AM MST

B. Domain Controllers - Thursdays, 1:00 AM MST

C. SQL Server (OS patches only) - Sundays, 1:00 AM MST

D. Web Application Servers – Sundays, 1:00 AM MST

E. All Other Servers – Saturdays, 1:00 AM MST

F. Network Hardware – Sundays, 2:00 AM MSTINAL

VIII. POLICY REVIEW AND UPDATE

This policy will be reviewed annually or as needed in response to significant changes in the technology environment or operational needs. Revisions will be made to ensure continual alignment with industry best practices and regulatory requirements.

Approved By:

Kate M. Fox 7/29/24

Kate M. Fox, Chief Justice **Date**
Chair, Wyoming Judicial Council