

Information Technology Resource Management Council (ITRMC)

ENTERPRISE POLICY – P4500 COMPUTER AND OPERATIONS MANAGEMENT

Category: P4520 – PATCHING & VULNERABILITY MANAGEMENT

CONTENTS:

- I. Authority
- II. Abstract
- III. Definition
- IV. Reference
- V. Policy
- VI. Procedure Reference
- VII. Contact Information
- VIII. Time Line
- IX. Revision History

I. AUTHORITY

Authority: Idaho Code § 67-5745(C)(3)

II. ABSTRACT

Establish the policy for state government organizations to establish patch and vulnerability management processes to proactively prevent the exploitation of IT vulnerabilities. Most major attacks in the past few years have targeted known vulnerabilities for which patches existed. To prevent such attacks from being successful, agencies shall create a systematic, accountable, and documented process to manage their exposure to vulnerabilities through the timely deployment of patches and other remediations.

III. DEFINITION

Agency – All state departments, boards, commissions, councils and institutions of higher education; but not elected constitutional officers and their staffs, the legislature and its staff, or the judiciary (per Idaho Code, 67-5745 [A]).

Application – Any data entry, update, query, or report program that processes data for a user.

Patch – Additional pieces of software code developed to address problems (commonly called “bugs”) in software.

Remediation – The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are: installing a patch, adjusting configuration settings, or uninstalling a software application.

Risk – The probability that a particular threat will exploit a particular vulnerability.

Risk Management – The process of identifying, assessing, and reducing risk to an acceptable level and implementing the right mechanisms to maintain that level of risk.

System – A computer, server, or IT device (e.g. router, switch, gateway, firewall) to include the hardware, operating system software, and installed applications.

Threat – Any circumstance or event, deliberate or unintentional, with the potential for causing harm to a system.

Vulnerability – A flaw in the design or configuration of software that has security implications. A vulnerability can be exploited by a malicious entity to gain greater access or privileges than is authorized.

IV. REFERENCE

ITRMC Guideline G570, *Patching and Vulnerability Management*

NIST Special Publication 800-40 (version 2.0), *Creating a Patch and Vulnerability Management Program*

V. POLICY

1. Each agency shall establish a systematic patch and vulnerability management process. At a minimum, this process, shall include the following:
 - A. Create and maintain an inventory of the agency's IT systems to determine which hardware equipment, operating systems, and software applications are used and require protection;
 - B. Regularly monitor security resources for vulnerability announcements and patch and non-patch remediations that correspond to the applicable operating systems and software within the agency's inventory;
 - C. Prioritize vulnerability remediation based upon the threat and potential impact on the agency;
 - D. Mitigate vulnerabilities, using patch and/or non-patch remediation, in a timely manner based upon the agency's prioritization.

- i. At a minimum, vulnerabilities must be mitigated no later than 10 business days from the time the vendor announces a remediation method.
 - 1. If an agency elects not to mitigate a known vulnerability within the 10 day time period, the agency's IT management must evaluate the risk of delaying remediation and document the decision to delay or avoid remediation.
 - ii. Each agency shall review and implement remediation actions described in the Multi-State Information Sharing and Analysis Center (MS-ISAC) security bulletins.
 - 1. These bulletins are sent on a timely basis to the primary and alternate Agency IT Security Coordinator from the Statewide Cyber Security Coordinator.
 - 2. Agency IT Security Coordinators must report compliance with the recommended remediation actions to the Statewide Cyber Security Coordinator no later than 10 business days from the time the Agency IT Security Coordinator received the MS-ISAC advisory.
 - a. If the agency elects not to implement the remediation actions due to extenuating circumstances (e.g. risk management decision, need for additional testing, etc), this decision must be communicated to the Statewide Cyber Security Coordinator. The Statewide Cyber Security Coordinator will then work with the agency to ensure adequate protections are in place to minimize any risks resulting from such a decision and will set a mutually agreed upon date for when said remediation actions will be completed (as applicable).
- E. Confirm the remediation actions have been applied appropriately by using one of the following methods:
- i. Verify the files or configuration settings have been changed as stated in the vendor's documentation for the specific remediation;
 - ii. Scan the system with a vulnerability scanner that is capable of detecting the known vulnerability;
 - iii. Verify whether the recommended patches were installed properly by reviewing patch logs; or,
 - iv. Perform a penetration test to attempt to exploit the specified vulnerability.

VI. PROCEDURE REFERENCE

When implementing patching and vulnerability management processes, agencies should consider the recommendations outlined within ITRMC Guideline G570 – Patch and Vulnerability Management Procedures.

VII. CONTACT INFORMATION

For more information, contact the ITRMC Staff at (208) 332-1876.

VIII. TIME LINE

Last Revised:

Effective Date: May 16, 2006

IX. REVISION HISTORY