BOISE STATE UNIVERSITY

University Policy 8050

Software Patch Management

Effective Date

October 2006

Last Revision Date

January 19, 2023

Responsible Party

Office of Information Technology, (208) 426-4357
Chief Information Security Officer, (208) 426-4127

Scope and Audience

This policy applies to all colleges, departments, and units, including all devices attached to the Boise State University network.

1. Policy Purpose

To protect the data and network-related resources of the University, to provide a secure and reliable network, and to reduce vulnerabilities on computers connected to the University network.

2. Policy Statement

Boise State University's network exists to support user's academic pursuits and the business needs of the University. Users are responsible for helping to minimize the potential for network disruption caused by their computer or electronic device. The Office of Information Technology (OIT) is ultimately responsible for Software Patch Management of electronic devices on the Boise State University network.

3. Definitions

3.1 Best Practices

Data management and network procedures generally recognized by the industry for assuring secure, reliable, scalable, and efficient data repositories and networks.

4. Requirement for Automated Patch Management

a. All university-owned computers that are connected to the network must be configured and tied-back to the OIT centralized patch management systems for action, reporting, and alerts. Mobile devices must be configured to receive automatic updates from their respective manufacturers. Other network devices, including printers and internet of things (IoT), must be updated according to the vendor patch schedule.

b. OIT is responsible for monitoring all devices for out-of-date version levels. All devices must be configured to allow for security scanning.

c. Firmware is updated when commissioned, upon subsequent recommissioning, or when a significant vulnerability is identified.

d. Any device that does not meet the above criteria, or that has met the vendor's end-of-life support status, must apply for an exception and must have a plan for risk mitigation and replacement, as outlined in section 7.

e. Colleges, departments, or units wishing to manage separate automated patch management platforms may apply for an exception, as outlined in section 7. If an exception is approved, the college or department will assume full responsibility for managing the electronic devices they propose to patch manage.

5. Best Practices

The University Technology Advisory Group will review and adopt appropriate standards and procedures that represent Best Practices with regard to the acquisition, implementation, management, and replacement of IT resources.

6. Responsibilities

The Chief Information Security Officer (CISO) is responsible for administering this policy, including its maintenance and compliance. A subcommittee consisting of the OIT Systems

Engineering Group and Client Computing Groups will review this policy and the minimum standards periodically and make recommendations regarding additions, deletions, and/or modifications to the CISO. Others wishing to make recommendations may make them directly to the CISO.

7. Exceptions to Policy

A Request for Exception, along with a plan for risk assessment and management, can be submitted for review by the CISO by completing a self-service support request. Non-compliance with these standards may result in revocation of access, notification of supervisors, and reporting to Internal Audit and Advisory Services and Institutional Compliance and Ethics.

8. Enforcement

a. Violations of this policy will be handled consistent with University disciplinary procedures applicable to the relevant individuals or departments. Failure to comply with this policy may also result in the suspension of access to network resources until policy standards have been met.

b. Should Boise State incur monetary fines or other incidental expenses from security breaches, the University may recoup these costs, as reasonable and appropriate, from the non-compliant department, school, or auxiliary organization.

9. Related Information

Minimum Security Standards for Systems
https://www.boisestate.edu/oit/itgrc/it-standards/minimum-security-standards-for-systems/

Request for Exception (self-service support request)
https://boisestateproduction.service-now.com/bsu_sp

Last Review Date

November 05, 2024

Revision History

January 19, 2023