BOISE STATE UNIVERSITY

University Policy #8050

Software Patch Management

Effective Date

October 2006

Responsible Party

Vice President and Chief Financial Officer, (208) 426-1200
Office of Information Technology, (208) 426-4357

Scope and Audience

This policy applies to all colleges, departments, and offices of Boise State University, including all devices attached to the Boise State University backbone, and is meant to enhance the academic and business functions of the University.

1. Policy Purpose

This policy was created to protect the data and network-related resources of the University, to provide a secure and reliable network available twenty four-hours a day, seven days a week in which end-users have confidence, and to reduce the vulnerabilities on computers connected to the university network.

2. Policy Statement

Boise State University's network is provided to users for the support of academics and the business of the University. Every user is responsible to minimize the potential for disruption of the network by their computer or electronic devices. The Office of Information Technology (OIT) is ultimately responsible for Software Patch Management of electronic devices on the Boise State University network.

2.1 Requirement for Automated Patch Management

All electronic devices attached to the university network will be configured to be automatically updated with patches that are identified as required by a patch management sub-committee of the university Network Administrators Group.

2.2 Centralized Network Administrators' Group

OIT will provide the service of automated patch management, available currently to the majority of electronic devices on the university network. As technology improves further automation may allow for support of all electronic devices, but the main focus for OIT will be to provide patch management to the greatest number of vulnerable devices.

2.3 Decentralized Patch Management

Colleges or departments may provide separate automated or rigorous and regular patch management. The colleges or departments will coordinate with the Executive Director, Information Technologies. The college or department will assume the full responsibility for managing the electronic devices that they propose to patch manage.

2.4 Patch Management Sub-Committee

A sub-committee of the Network Administrators Group will be formed and will be charged with the task of maintaining a standards document on the minimum patch level for Operating Systems at the university.

2.5 Best Practices

OIT, and the colleges and departments operating de-centralized patch management systems, will seek and adopt whenever possible best practices with regards to the deploying and providing patch management. The Network Administrators Group shall review and adopt appropriate standards and procedures that represent best practices.

3. Responsibilities and Procedures

3.1 Modification of Policy

a. The Executive Director of Information Technology (IT) is responsible for administering this policy, including its maintenance and compliance.

b. A subcommittee of the Network Administrators Group (the Network Policy Subcommittee) will review this Policy periodically and make recommendations regarding additions, deletions

and/or modifications to the Executive Director of IT. Others wishing to make recommendations may make them directly to the Executive Director of IT.

3.2 Exceptions to Policy

a. Any college, department or office that wishes an exception to this policy must present its written request to the Patch Management Subcommittee.

b. The Patch Management Subcommittee will review and forward the request with the Subcommittee's recommendation to the Executive Director of IT. The Executive Director of IT will then either approve or deny the exception. The Subcommittee's recommendation and the decision from the Executive Director of IT will be forwarded to the requesting party within thirty days.

c. Only the Executive Director of IT may authorize an exception to this policy.

3.3 Procedures

3.3.1 Non-Compliance with this Policy

If the university Network Engineer determines that the university is at risk, or if the Network Engineer initiates an automated compliance system, the identified offending electronic device will be disconnected from the university network.

If no risk is determined, then;

3.3.1A First Offense

Non-compliance with this policy will result in a warning notice being sent by the Network Administrators Group Chair to the responsible System Administrator by e-mail or letter. The warning notice shall include a description of the violation referencing the Network Policy and recommending the necessary corrective action and acceptable time frame for required actions to be completed.

3.3.1B Second Offense

A second offense of non-compliance with this policy will result in a warning notice of non-compliance from the Network Administrators Group Chair to the responsible System Administrator with copies to the appropriate Dean or Director and the Executive Director of IT. The warning notice shall include a description of the violation referencing the Network Policy and requiring immediate corrective action.

3.3.1C Continued Offences

A third violation of this Policy will result in the disconnection of the offending electronic device from the university network. The Executive Director of IT will direct a notice to the appropriate Dean or Director with a copy to the IT Governance Council. Such services will not be re-established until the Network Subcommittee notifies the Executive Director of IT that the violation has been resolved in accordance with established policy.

Revision History