



Policy Number:	5.002
Originating Office:	Information Technology Services
Responsible Executive:	Vice President for Administration and Technology
Date Issued:	02/03/2011
Date Last Revised:	08/05/2015

Patch Management

Policy Contents

- I. Reason for this Policy.....1
- II. Statement of Policy1
- III. Definitions.....2
- IV. Procedures2
- V. Related Documents, Forms and Tools.....2

I. REASON FOR THIS POLICY

The University of South Dakota has established a formal policy and supporting procedures regarding security update deployment to ensure the confidentiality, integrity, and availability of University data and information systems. Timely application of security updates decreases the number of common vulnerabilities affecting University-owned computing equipment. This policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding the University of South Dakota's needs and goals. This policy also ensures that USD meets the requirements for the Payment Card Industry Data Security Standards (PCI-DSS).

Policy last reviewed 8/5/15 by the CIO Management Team

II. STATEMENT OF POLICY

This policy applies to all University-owned computing equipment including but not limited to those systems used to store, process, or transmit cardholder data. All University-owned computing equipment must comply with the following:

1. Licensed operating system software must be utilized for all University-owned computing equipment and system components.
2. No user shall disable or tamper with the configuration of security updates on University-owned computing equipment.
3. All desktop and laptop computers must have security updates set to update automatically.

4. All servers must have an adequately staffed process for regularly reviewing and installing security updates, bug fixes, or upgrades.
5. Exceptions to this policy must be approved by the Vice President for Administration and Technology.

III. DEFINITIONS

Computing Equipment: Computing devices that utilize the wired or wireless network to transfer data; including, but not limited to, desktop computers, laptops, tablets, smart phones, and game consoles.

Network Service: A software application which provides access to a resource via network requests from computing equipment; including, but not limited to, file and printer sharing, web servers, and Dynamic Host Configuration Protocol (DHCP) servers.

Server: Any computer or device whose purpose is to provide a network service or storage to computing equipment.

IV. PROCEDURES

Computers will be loaded with the standard supported operating systems. Supported options can be found at <http://www.usd.edu/technology/computer-requirements>.

Windows updates will be configured to run every Wednesday by 5:00 am.

Security patches for servers are reviewed and installed as necessary by the server team on a quarterly basis.

V. RELATED DOCUMENTS, FORMS AND TOOLS

Not Applicable