	Policy: IT Division Resource Patch Policy	No. 2010-1	Rev. 01/11/2010
		Date Approved:	03/10/2010
		Authors:	Stephanie Fuller
		Filename:	IT Division Resource Patch Policy

WSU IT DIVISION RESOURCE PATCH POLICY

I. Purpose

System resource patching is a critical part of data protection and security. Computer systems need to be prepared against the constant and dynamic threats to system flaws that may cause interruptions of service and malignant attacks that may steal or corrupt data. Documenting the patch schedule promotes division and campus-wide recognition of the need and value to the campus user community. Documenting the patch schedule also communicates awareness of patching to application stake holders, system engineers, DBAs and the IT Community. It also documents that systems are current.

II. Scope

This policy applies to all systems managed by the IT Division or under an active SLA with the IT Division.[1]

III. Definitions

Application owner/stakeholder - Campus representative who owns the application.
Operating System – Winows or Unix system running on a computer to support an application.
Windows – A Windows system running on a computer.
Unix - Solaris, RedHat, SuSE, MacOSX, OES, SLES
Databases - Oracle, MSSQL, PostGRES, MySQL
Application vendor support - Vender certification of application on given system platform/patch level or database revision.
Semester – WSU semester calendar

[1] The IT division highly recommends all university technology resources comply with this patch policy to mitigate risk and improve data and network security.

IV. Standards

Different systems require different patching schedules based on the frequency of changes published and the security threats that arise.

- OPERATING SYSTEM PATCHING

UNIX system administration assesses the need to upgrade or patch the operating systems every semester. Every effort should be made to keep systems to industry accepted current system levels and vendor recommendations.

Windows system administration assesses the need to upgrade or patch systems in accordance with the monthly Microsoft patch cycle.

- DATABASE PATCHING

Database Administration assesses the need to upgrade or patch databases every semester. The decision to apply patches or upgrades will be dependant on the application needs, the severity of the patch and application vendor support.

- APPLICATION PATCHING

Application owners assess the need to upgrade or patch applications then submit a request for change to the IT Division Change Control Process.

- NETWORK

Network administration assesses the need to upgrade or patch network device software at least annually per industry recommendations.

- TESTING

Patches will be applied on test systems prior to installation on production systems.

- URGENT PATCHES

Unplanned upgrades and patches may become necessary to address a critical bugs, security vulnerabilities, or added features.

Critical bugs and new features are announced by vendors. System administration engineers will assess the need for applying bug fixes. These will be applied as soon as possible coordinating with the application owner via the change management board.

System and network administration engineers assess the need for patching to resolve security vulnerabilities discovered by monthly security scans. When high and severe vulnerabilities are reported, they will be resolved either by patching or mitigating the effect of the reported vulnerability within 30 days.

- SCHEDULING AND REPORTING

Patch scheduling and necessary system outages should be scheduled in accordance with the Change Control Policy. Successful patch completion should be documented in accordance with the Change Control Policy.

- REVIEW AND REVISION

Review of and compliance with this patching policy will be reviewed at least annually by the Change Management Board.

V. Procedures

Because every system will have unique requirements that will affect the method patches are applied, individual procedures will be the responsibility of the person applying the patches – System Engineer, Database Administrator or Network Engineer.

VI. Roles/Responsibilities

Application Owner/Stake Holder

- Determining need for and applying application patches or upgrades.
- Requesting application patch or upgrade by appropriate DBA or engineer.
- Allow reasonable outages for system engineers or DBAs to apply patches and upgrades in a timely manner.

System Engineers

- Assessing need for applying operating system patches.
- Reviewing monthly security reports and patching or mitigating the reported vulnerabilities.
- Monitor vender announcements of critical bugs.
- Scheduling system outages with the change advisory board (or change management board).
- Applying the necessary patches.
- Updating the change management board when patches are completed.

Data Base Analysts

- Determining need for and applying Oracle patches and upgrades.
- Scheduling database and application patches with the change advisory board.

- Updating the change management board when patches are completed.

Change Advisory Board

- Notify necessary stake holders when patching/upgrading is requested.
- Documenting when patching is completed.

Information Security Office

- Review this policy annually and update it as required.

VII. References

Change Control Policy (Proposed)
Information Security Roles and Responsibilities (PPM 10-1)

VIII. Approved By

IT Council

IX. Revision and Review History

Date	Version	Description
12/4/2009	1.0	New Policy Created