



# Gonzaga University Information Technology Policy and Procedure

**SUBJECT: Vulnerability Remediation**

Policy Number	Date Issued	Date Reviewed
IT108		

**PURPOSE:**

Gonzaga University is committed to the routine maintenance of its computing assets. As such this policy is put forth to provide guidance in the routine patching of software and operating systems.

**SCOPE:**

This policy applies to all equipment that is owned, leased, operated, maintained, or connected to the Gonzaga University network, including personally owned equipment.

**POLICY:**

Patches and service packs will be applied to workstations and servers in order to remediate exposure to applicable security issues.

A patching software package (PSP) will be utilized to centralize the administration, installation, tracking and reporting of patches.

Patches and service packs will be identified for appropriateness and tested to the extent possible prior to installation.

Patches and service packs will be installed on target machines in a timely fashion.

Servers will be patched and maintained by the lead technician assigned to the respective device.

**DEFINITIONS:**

*Analyze* – Through this process, current patch levels must be determined and a minimum baseline policy should be defined.

*Critical Update* – This is not a security update but a fix for any issues in broadly applied software. Usually publicly available and have an accompanying Knowledge Base article.

*Discover* – This phase in PSP Patch Manager involves locating assets (workstations and servers) on the network and categorizing them.

*Driver Update* – Update to software that supports and controls hardware. Driver updates may come from the software or hardware vendor.

*Feature Pack* – Software package that includes non-critical additions to the base software program. It typically appears between major releases.

*Hotfixes* – Patches built to address specific issues. Recipients may not distribute hotfixes outside their organizations without written authorization from Microsoft. Hotfixes do not receive the same testing process.

*Lead Technician* – The technician responsible for a specified grouping of target machines.

*Remediate* – To “remedy” the vulnerabilities found by bringing systems up to date, best accomplished via policy based solutions.

*Report* – Reporting conducts a change review and verifies successful deployment of patches. Reporting should also include enough review, analysis, and adjustment to close the loop and begin cycle again automatically (see Patch Management Best Practices)

*Research and Test* – In this phase of patch management, missing service packs, patches and any other software updates must be investigated and understood. A risk analysis must be done for missing patches.

*Security Update* – Update that corrects a known security flaw, there is a severity rating included with each update, as is a security bulletin discussing the issue and a Knowledge Base article describing the patch in detail.

*Service Packs* – are cumulative packages of hotfixes, security updates, critical updates and updates. A service pack undergoes both internal and external testing.

*Software Update* – is any update, update rollup, service pack, feature pack, critical update, security update or hotfix.

*Target Machine* – A computer identified as requiring a patch, service pack or other update.

*Update* – addresses a non-critical, non-security issue.

*Update rollup* – cumulative package of hotfixes, security updates, critical updates, and updates, collectively tested for easy deployment.

*Upgrade* – software that updates and upgrades a piece of software to a newer version while keeping the settings and data from the prior program.

## **PROCEDURE:**

- I. In general, the patch management system will be administered centrally with certain responsibilities managed by technicians throughout the University.
- II. Patches will be downloaded on a monthly basis to the PSP server by the Asset Manager.
  - a. The Asset Manager will ensure that all patches download successfully and that the local server validates each patch.
- III. Patches will be tested locally prior to widespread release.
  - a. Patches should be tested within 5 working days of release for regular-cycle patches and 2 working days for out-of-cycle releases.
  - b. Patches should be applied only after testing and confirmation of readiness and appropriateness.

- IV. Prior to the release of any patches, the Asset Manager will perform a campus-wide computer discovery using PSP to locate any new computers.
- V. When a patch has been tested and marked as ready for release, and the computer discovery is complete, the Asset Manager will notify all technical staff.
- VI. The Asset Manager will deploy tested patches to machines on a subnet by subnet or department by department basis.
- VII. The Asset Manager will record problems in the Help Desk Management Software, the lead technicians in each area will be responsible for resolving any issues that arise as a result of the patch deployment.
- VIII. The Asset Manager will communicate to technical staff as each patch deployment is complete.
- IX. The Asset Manager will provide detailed deployment reports upon request.

**PROBLEM MANAGEMENT**

- I. The technician who discovers the problem will immediately report problems to the Help Desk (tickets will assigned to the Asset Manager).
- II. Tickets will include:
  - a. Details of problem and symptoms.
  - b. Troubleshooting steps.
  - c. Extent/configurations on which the problem was encountered.
- III. The Asset Manager will work with the lead technician to resolve problem(s).
- IV. Depending on scope, the Asset Manager will determine whether to stop implementing the particular patch.

**ENFORCEMENT:**

Any University personnel found to have violated this policy may be subject to disciplinary action, at the discretion of their supervisor, as described in the university's **Personnel Policies and Procedures Manual**.

<b>Date:</b>	<b>President or Designee</b>