



Gonzaga University Information Technology Policy and Procedure

SUBJECT: Student and Visitor Anti-virus Protection

Policy Number	Date Issued	Date Reviewed
IT602		

PURPOSE:

The purpose of this policy is to ensure that any student or visitor computer that is to be connected to the university's data network, including those not owned by the University, is properly maintained with all current system and application patches from software vendors and is running an effective anti-virus application which is using current virus definition files. The policy is designed to minimize the potential exposure to Gonzaga University from damages which may result from un-patched or unprotected computers which are connected to the campus data network.

As such, it is the responsibility of each member of the university community to ensure that they use that resource responsibly, that their network traffic is consistent with the university's **Acceptable Use Policy**, and that they do not place other users or their computers at risk of harm.

SCOPE:

This policy applies to all students and visitors who wish to connect their computers to the campus data network.

POLICY:

All students and visitors will only access the network with computers that are properly maintained with the most recent operating system patches, critical updates, security updates, service packs, and updates.

All students and visitors will only access the network with computers that have applications installed that are properly maintained with up to date critical updates, security updates, service packs, and updates.

All students and visitors will have installed anti-virus software that is functioning and up to date with the most recent virus definition files current prior to accessing the Gonzaga University network.

DEFINITIONS:

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.

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.

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. Enforcement

- a. The network services staff will be charged with enforcement of this policy.
- b. Violations will be determined by traffic studies and other measures deemed appropriate.
- c. Any device exhibiting a pattern consistent with a known virus or other type of mal-ware or any machine consuming excess network/IT resources such that it interferes with other network users or services will be considered in violation of this policy.
- d. The Network Manager is the final appeal in all disputes arising from this policy.

II. Sanctions

- a. Visitors:
 - Any visitor found to be in violation will be barred from connecting to the university's campus network until such time as they can demonstrate to ITS staff that they are in compliance with this policy.
- b. Students
 - First Offense - Any student found to be in violation will be barred from using the university's campus network until such time as they certify to ITS staff that they are in compliance with this policy.
 - Subsequent Offenses – Any subsequent offense will result in that student's machine being barred from the residence hall and courtesy network for a period of one week.
- c. Students attending the School of Law must refer to the **Mandatory Virus Protection & Windows Patches** policy for the appropriate sanction schedule.

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**.

Date:	President or Designee