



Gonzaga University Information Technology Policy and Procedure

SUBJECT: Virus Protection and Prevention

Policy Number	Date Issued	Date Reviewed
IT105		

PURPOSE:

Gonzaga University is committed to ensuring the integrity of its information technology (IT) assets from malicious software including virus, trojans, spyware, and other harmful code. As such, this policy is put forward to ensure the integrity of IT assets.

SCOPE:

This policy applies to all faculty, staff, temporary employee, and other personnel within Gonzaga, including employees of affiliated third-party organizations. This policy applies to all equipment that is owned, leased, operated, maintained, or connected to the Gonzaga University network, including personally owned equipment (see **Student and Visitor Anti-Virus Policy**).

POLICY:

Gonzaga University will employ an enterprise virus protection software package.

The university will always run the supported anti-virus software on all servers and workstations attached to the network.

Virus definitions and software updates will be downloaded from the service provider as they become available.

All client workstations will run enterprise virus protection software when possible. If enterprise virus protection software is not available, alternative virus protection software is required.

Other virus protection software or utilities may be utilized if necessary provided that these software packages do not interfere, denigrate, or disable the enterprise software package.

DEFINITIONS:

Hacker - One who uses programming skills to gain illegal access to a computer network or file.

Virus – Malicious program or code written by a hacker.

Virus Definition – Software code that uses flags, binary indicators, and/or Bayesian technology to identify viruses.

PROCEDURE:

- I. The University standard, supported anti-virus software, available from the corporate download site will be automatically downloaded, installed, and updated as they become available. Some servers may be exempted from this policy.
- II. Users should NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- III. Delete spam, chain, and other junk email without forwarding, in with compliance with the Gonzaga Acceptable Use Policy.
- IV. Never download files from unknown or suspicious sources.
- V. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- VI. Always scan a floppy diskette or any other removable media from an unknown source for viruses before using it.
- VII. Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- VIII. If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

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