FERRIS STATE UNIVERSITY

BUSINESS POLICY

Antivirus Software Requirement for Computing Devices

Effective Date:	12/01/2014
Policy Number:	2015:05
Policy Owner:	Chief Technology Officer, Information Technology Services (ITS)
Supersedes:	Antivirus Policy

SCOPE

This policy covers all computing devices, including those owned by students, faculty, staff, contractors, and affiliates, that connect to the Ferris State University network via standard network, cellular, wireless, or modem connections.

POLICY STATEMENT

All University owned computing devices (laptops, desktops, servers, smartphones, tablets, etc.) connected to Ferris State University's secure networks will have the University standard, centrally managed antivirus software installed.

All personally owned computing devices connecting to secure Ferris networks will be required to have one of the antivirus software programs approved by Ferris Information Technology Services. If the device does not have an approved, up-to-date antivirus software installed and enabled, the device will be granted limited network access so that the user can access the resources needed to remedy the situation.

In the event that no antivirus protection is available for a particular operating system or platform (i.e. smartphones and tablets), anyone using or accessing these unprotected systems shall apply all prudent security practices to prevent infection. These security practices include the application of all essential patches as soon as they become available.

If ITS personnel identify a virus or malware-infected computing device that may be a threat to network operations, computing resources, or information security, they will take immediate action to block the device from using the network until it is verified by our standard tools to be virus and malware-free.

Any exceptions to this policy must be approved in writing by the Chief Technology Officer.

Violations/Sanctions

Suspected or known violations of this policy or applicable laws must be reported to Information Technology Services (TAC Service Desk), and if applicable, an employee's supervisor. Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by current University policy, student code of conduct, and/or collective bargaining agreements. When appropriate, University authorities and/or law enforcement agencies may conduct an investigation into the incident.

DEFINITIONS

Antivirus software

Software that runs on a computing device that scans, monitors, and protects the device from being infected by viruses and malware. Antivirus software is generally reactive. This means that for each new virus discovered, the software vendor must develop a “virus definition” or “signature” file, so that the antivirus software can recognize the new virus.

Compensating Control

An alternative, but effective, means of meeting a goal or requirement. Compensating controls may be considered when a requirement cannot be meet explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls.

Computers/computing devices

For the purposes of this policy, computers or computing devices are any type of electronic device that sends and receives data on our network that could become infected with a computer virus or malware. Examples of computing devices would be, but are not limited to, workstations, servers, desktops, laptops, mobile computing devices, smartphones, tablets, etc.

Malicious software (Malware)

Any type of computer code or software program designed to do damage or other unwanted actions on a computer system is considered malware. Common examples of malware include viruses, worms, Trojan horses, and spyware. Spyware can gather data from a user's system without the user knowing it. This can include anything from the Web pages a user visits, to personal information such as credit card numbers, social security numbers, and passwords.

Virus

Viruses are a “subset” of malware. Like a biological virus, a computer virus is something that is often detrimental to the health of a system. Computer viruses are often small programs or scripts that have malicious intent, and can create files, move files, erase files, erase entire directories, or fill a computer's memory causing the computing device to function incorrectly. Opening an infected e-mail attachment is the most common way to get a virus. Viruses can be transmitted via e-mail or instant messaging attachments, files downloaded from the Internet, CDs, and other removable media. Viruses are usually disguised as something else, and their presence is not always obvious to the user.

Virus definition files

Files provided by vendors to update their antivirus software to recognize and deal with newly discovered malicious software. Since new viruses are created every day, definition files need to be updated frequently—having out of date virus definition files leave the computing device vulnerable to new viruses.

Computing Resources

Servers, applications, and services managed or used under contract by Ferris State University

Secure Ferris Networks

Any networks Ferris has set up that require authentication with a Ferris Computing ID and password to access. Ferris Public Wi-Fi is not a secure network.

RESPONSIBILITIES

The following responsibilities are illustrative and not meant to be an exhaustive list.

Information Technology Services (ITS)

- ITS will take appropriate action to contain virus infections. This may include disconnecting a suspect computing device from the network, blocking a device from accessing our resources, or disconnecting an entire segment of the network.
- ITS staff will follow internal processes, policies, and procedures related to the handling of virus outbreaks, as spelled out in the *FSU IT Security Incident Process* and related documents.
- ITS will attempt to notify our community of any credible virus and malware threats.

For University owned computing devices:

- ITS will keep the antivirus products it provides up-to-date, including the virus definitions and software client.
- ITS will install antivirus software on all Ferris State University owned desktops, laptops, servers, and other devices as appropriate. The most up-to-date version of the approved antivirus software will be used as the default standard.
- ITS will configure the management console of the antivirus software to check the manufacturer's site for new virus definition files, push them to University owned computers at regular intervals, and balance the need for security while not interfering with the operation of the computing devices.
- ITS will take appropriate action to contain virus infections and assist in the recovery from virus infections on computing devices in our scope of control.

For personally owned computing devices:

- ITS will assist employees and students in the installation of antivirus software according to standards on personally owned computers. There usually is a fee for this service.
- ITS will provide licensed copies of our approved antivirus software for any University employee's personal devices as available through University software contracts.

User Responsibilities

The responsibilities of any user of Ferris computing resources and the network include:

- Taking reasonable measures to protect your computing devices against virus and malware infection. Information on protection against viruses and malware can be found on the Ferris My Tech Support website.
- Not attempting to alter or disable antivirus software on any University owned computing device without the expressed consent of the ITS department.
- Ensuring that a Ferris approved antivirus software program is installed on any personally owned devices used to access the Ferris State University network as appropriate for the operating system/platform as well as installing appropriate operating system/platform security patches.

Additional responsibilities of Ferris employees and affiliates:

- Notify ITS (by contacting the TAC) to arrange for evaluation, development, and implementation of agreed upon compensating controls if they encounter or expect interference between the antivirus software and another business related application running on University owned computing devices.
- Uninstall the University licensed antivirus software from their devices after their employment or volunteer term with the University has ended.

Additional responsibilities of Ferris students:

- Obtain and install one of the approved antivirus programs listed on the Desktop and Classroom Standards Committee or on the My Tech Support web site.
- Remove viruses from their devices, or bring it to Student Technology Services to have viruses removed (there is a fee for this service).

CONTACTS

For all questions related to removing a virus, obtaining antivirus software, exceptions, etc. Please contact TAC at 231-591-4822 or toll free at 877-779-4822 or by email at tac@ferris.edu.

RELATED INFORMATION/FORMS/INSTRUCTIONS

Ferris Policies

Please see the University Business Policy site for related policies, guidelines, and more
http://www.ferris.edu/HTMLS/administration/buspolletter/
Information Security Policy
http://www.ferris.edu/HTMLS/administration/buspolletter/Bpl1104.pdf
Information Security Guidelines
http://www.ferris.edu/htmls/administration/buspolletter/Bpl0907InfoSecurityGuidelines.pdf
Proper Use of Information Resources, Information Technology, and Networks Policy
http://www.ferris.edu/htmls/administration/buspolletter/Bpl9607.htm
FSU IT Security Incident Response Process (Ferris internal document with restricted distribution)

Related Websites:

My Tech Support web site
http://www.ferris.edu/techsupport
Desktop and Classroom Technology Committee web site
http://www.ferris.edu/HTMLS/tatfsu/technicalstandards/Index.htm