

Information Security Policies

Antivirus Policy

Version: 1.0

Effective Date:

9-23-11

Approved by:

IT Advisory

Committee

Antivirus Policy

1.0 Purpose

To establish requirements which must be met by all computers connected to Keuka College networks to ensure effective virus detection and prevention.

2.0 Scope

Individuals affected:

This policy applies to all students, faculty, and staff attending or employed by Keuka College who access, handle, use or otherwise connect to the college's information technology resources (also referred to as *users*). In addition, the designation user also refers to all visitors, subcontractors, potential students, research associates, media representatives, and non-college entities or individuals who are granted access to Keuka College's information technology resources.

Resources covered:

This policy applies to all computers that are Apple Computer or PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers, and any PC based lab equipment such as traffic generators. This applies to all Apple Computer or PC-based computers whether individually controlled, shared, stand alone or networked. It applies to all computers and communications devices owned, leased, operated or provided by Keuka College. This includes, but is not limited to personal computers, wireless communication devices, networking devices, workstations, servers, and any peripheral devices and the associated software thereof. This policy also applies to all privately owned devices used to store, process or transmit college owned data.

3.0 Policy

All Keuka College Apple Computer or PC-based computers must have one of Keuka College's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Information Technology Service (ITS) Support Personnel are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious software into Keuka College's networks (e.g., viruses, worms, Trojans, botnets, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

Noted exceptions: Machines with operating systems other than those based on Apple Computers or Microsoft products are exempt at the current time.

4.0 Enforcement

Compliance:

At minimum these principles must be followed by individuals while connected to Keuka College resources. Individual departments may apply stricter standards, provided they do not conflict with the standards and procedure outlined in this document.

5.0 Definitions

Information Technology Services (ITS) Resources – Any and all college resources, whether individually controlled, shared, stand alone or networked, and all computers and communications devices owned, leased, operated or provided by Keuka College. This includes, but is not limited to personal computers, wireless communication devices, networking devices, workstations, servers, and any peripheral devices and associated software.

Malicious Software – Malicious software is any program designed to abuse Information Technology Services resources or users.

Users – Faculty, Staff, Students, and other members of the Keuka college community that use or interact with the Keuka College network in any fashion.

6.0 Revision History

05/10/2011 – rev 1.0 – Document Created

7.0 Policy Impact Statement

All college systems vulnerable to attack by malicious software (malware) must be secured by antivirus software whenever possible unless a specific exemption has been given. Malicious software is self replicating and designed to destroy or corrupt information or adversely affect the usage of Information Technology Services (ITS) resources. A malware infection is almost always costly to an institution whether through loss of data, employee time to resolve, or the delay of work. Malware that originates from the college can lead to damaged reputation, potential litigation in addition to the employee effort required to investigate and repair. In light of the potential costs an antivirus policy is a solid investment in the security of Keuka College resources.