Anti-Virus Policy

Objective

The purpose of the Anti-Virus Policy is to establish the requirements for addressing Malware infection, prevention, detection and cleanup.

Applicability

The Anti-Virus Policy applies to all University students, faculty or staff members, whether full-time or part-time, paid or unpaid, temporary or permanent, as well as all agents and representatives of the University, including any third party service provider providing services to the University who create, use or otherwise access or interact with any University Information or University Information Resource ("University Users")..

Definitions

Malware: includes Virus, Trojan Horse and Worm.

University Information Resource: any tool, device, equipment, or system used to create, collect, record, process, store, retrieve, display and transmit University Information, including but not limited to email, mainframes, servers, computers, laptops, personal digital assistants (PDA), telecommunication resources, fax machines, printers, file cabinets, software and embedded technology.

Policy

- All University Information Resources, whether connected to the Suffolk University network, or standalone, must use the Information Technology Services (ITS) management-issued virus protection software and configuration.
- All other non-University Information Resources must use ITS management-approved virus protection software and configuration, prior to any connection to a University Information Resource. For example, if a user is connecting to the University network through a personal computer, the user's personal computer must use ITS management approved virus protection software and configuration.
- The virus protection software must not be disabled or bypassed.
- The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
- The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
- Each E-mail gateway must utilize Suffolk University ITS management approved email virus protection software and must adhere to the Suffolk University rules for the setup and use of this software, which includes but is not limited to scanning of all inbound and outbound emails.
- Every Malware that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported. A user may become aware that a virus has not been automatically cleaned upon receipt of a pop-up message from the virus protection software.

In the event a user suspects that any University Information Resource may be infected by a virus, please contact the University's ITS Helpdesk immediately at 617-557-2000.

Violation of Policy

The University reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with this Policy. Violations of this Policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this Policy may result in dismissal from the University.

Revision History

Version	Date	Responsible University Office	Approved By
1.0	09/14/10	Provost Office	Provost Barry Brown