University *of* New Haven

Policies and Procedures

Policy Title: Office of Information Technology Asset Protection

Policy No.: 7030 Rev.: 0
Effective Date: November 14, 2014
Last Revision: November 14, 2014

Responsible Office: Office of Information Technology
Responsible Official: Associate Vice President for Technology & CIO

Contents

Scope

It is expected that implementation of the control mechanisms defined in this policy will mitigate the risks and losses associated with security threats to the University's assets.

Policy Statement

One of the Office of Information Technology's (OIT) priorities for the University is to provide and maintain a safe and secure computing environment. OIT incorporates several control mechanisms to ensure University assets are protected from threats. It is a violation of policy for anyone to engage in any activity which threatens university asset security. Such activity can include, but is not limited to the creation of computer viruses, malware, adware, spyware, or

Trojan programs.

Reason for the Policy

The purpose of this policy is to establish the requirements and responsibilities for the assets that are managed by OIT in providing overall security to the University's information technology resources

Definitions

Spyware
Software that is installed in a computer without the user's knowledge and transmits information about the user's computer activities over the Internet.

Trojan
A program that appears legitimate, but performs some illicit activity when it is run.

Virus
A computer program that can copy itself and infect a computer without permission or knowledge of the user.

Malware (Malicious Software)
Software designed to infiltrate or damage a computer system without the owner's informed consent.

Adware (Advertising-supported software)
Any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used.

Control Server
A central console used for monitoring, reporting and updating remote computers.

OIT
Office of Information Technology

Policy Sections

7030.1 Asset Protection Configuration

The Office of Information Technology protects all PC assets from viruses by Trend Micro's NeatSuite Enterprise solution software. All computers, laptops and servers have the latest engine and profile installed and updated via a Control Server. Spyware/Trojan protection is also provided by the client.

The Control Server monitors all infections and reports outbreaks. Remote scanning and/or regular scheduling of scans are available.

Exchange is protected by Trend Micro's ScanMail application. ScanMail is also monitored by the Control Server.

7030.2 Responsibilities

7030.2.1 Office of Information Technology responsibilities:

The Office of Information Technology has the responsibility of providing support and maintenance for the software used to secure the University's assets. The Office of Information Technology also will ensure that the Control Center remains updated with the latest virus and spyware definition files from Trend Micro. They will provide reports on infected/cleaned/quarantined systems as requested.

7030.2.2 Employee responsibilities:

Employees shall not knowingly introduce a computer virus into university computers, load diskettes of unknown origin or open attachments without first verifying the source. Incoming diskettes shall be scanned for viruses before they are read. Any employee who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the helpdesk at extension 8324.

Employees shall not knowingly allow spyware to install on university computers. Additionally, employees shall perform anti-spyware updates and run anti-spyware programs regularly, as directed by OIT. Any symptoms that suggest spyware may have been installed on your computer needs to be reported immediately.