POLICY NUMBER: IT-002
DIVISION: NET Services
POLICY: NSU Anti-Malware Policy
ISSUED BY: Chief Information Officer

Approval Date: 01/29/2009
Approved By: Senior Cabinet
Review Date: 07/12/2011
Review Date: 10/02/2012
Review Date: 02/20/2014
Review Date: 06/21/2016: Change to malware policy, update definitions
Review Date: 6/21/2017: No changes
Review Date: 9/10/2018: No Changes

INTRODUCTION

The National Institute of Standards and Technology (2005) defines malware as "a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim" (p. ES-1). Malware includes all software that has a malicious intent such as virus, worms, Trojans, backdoors, rootkits, bots and spyware.

A virus infection is almost always costly to the institution whether through the loss of data (possibly p ermanent), staff time to recover a system, or the delay of important work. Viruses spread from the U niversity can lead to damage to the University's reputation and can make the University vulnerable t o possible litigation that costs money and the staff effort necessary for investigation and remedy.

PURPOSE

The purpose of the Anti-Malware Policy is to describe the responsibilities of individuals, departments and NET Services in protecting the University from viruses.

TARGET AUDIENCE

The NSU Anti-Malware Policy applies to all NSU faculties, staff, students and guests who utilize the n etwork and other information technology resources owned and/or operated by NSU.

POLICY

NET Services Responsibilities

- To provide anti-malware licenses for all computers owned and operated by NSU
- To install anti-malware software on all basic computer images for faculty, staff and computer lab machines;
- To keep the anti-malware products up-to-date through a centralized policy management that allows for automatic deployment of new virus definitions;

- To take appropriate action to contain malware infections and assist in their removal. As such, NET Services retains the right to remove a suspect computer from the network or disconnect a segment of the network to prevent the spread of a virus or contain damage being done by malware;
- To disseminate information on general malware protection, including information on virus hoaxes;
- To assist users in the recovery from a malware attack, including advise on containment to stop the spread and assistance with malware removal;
- To maintain documentation on malware incidents, including prevention of recurrence;
- To maintain knowledge and expertise on malware and malware protection through routine staff training, awareness and access to resources;
- To perform periodic sweeps of server system files and staff file stores and conduct real-time scanning on all file and web servers;
- To provide malware protection for faculty and staff e-mail by scanning incoming mail before it is delivered, deleting infected attachments, and blocking potentially harmful files with certain file extensions.

Individual Responsibilities

- To take suitable measures to protect against malware infection by ensuring that anti-malware software is installed and properly functioning;
- To report to the Support Desk any suspicion of an infected machine.

Reference(s)

National Institute of Standards and Technology. (2005). *Special publication SP800-83: Guide to malware incident prevention and handling.* Retrieved July 14, 2016, from http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf