



POLICY NUMBER: IT-006
DIVISION: NET Services
POLICY: NSU Patch Management Policy
ISSUED BY: Chief Information Officer

Approval Date: 01/06/2009
Approved By: NET Services Coordinator's Council

INTRODUCTION

A virus is a piece of self-replicating code, most often a malicious software program designed to destroy or damage information on computers. Some viruses cause no damage apart from reproducing, but a significant number are specifically designed to cause data loss or to compromise the confidentiality of files by sending copies of them to others.

Potential sources of viruses include shared media such as floppy disks or CD-ROMs, electronic mail (including, but not limited to, files attached to messages), and software or documents copied over networks such as the campus network and the Internet.

A virus infection is almost always costly to the institution whether through the loss of data (possibly permanent), staff time to recover a system, or the delay of important work. Viruses spread from the University can lead to damage to the University's reputation and can make the University vulnerable to possible litigation that costs money and the staff effort necessary for investigation and remedy.

PURPOSE

The purpose of the Patch Management Policy is to define the responsibilities for the identification, implementation and documentation of information technology security patches.

TARGET AUDIENCE

This policy applies to all NSU administered computer equipment. Authorized systems that are supported outside of NET Services are the responsibility of the authorized administrator.

POLICY

- Administrators must monitor solutions for security patches through vendor bulletins, industry notification lists and/or application specific security tools.

- Administrators will assess the critical nature of vulnerabilities and patches as they become available and determine the urgency and timing based on the assessment.
- Administrators are responsible for the implementation of the upgrades to be applied. Should a critical security condition exist, systems may be rebooted immediately upon installation of the patch.
- NET Services staff will take appropriate action to contain security incidents and assist in resolving the problem. As such, NET Services reserves the right to remove a suspect computer from the network or disconnect a segment of the network.
- NET Services staff will communicate with appropriate university personnel regarding recent software security problems and recommend patches and security updates to reduce threat.