**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
Revision Date: No revisions
Review Date: 11/05/2010
Review Date: 07/02/2012
Review Date: 10/2/2012
Review Date: 2/20/2014 – Modified the introduction
Review Date: 6/21/2016 – No changes
Review Date: 6/29/2017 – No changes

---

**INTRODUCTION**
A patch is a piece of software that is designed to resolve problems with a particular computer program or to update the program. Often, a patch fixes security vulnerabilities. A patch management policy is part of a comprehensive security plan.

**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.