



POLICY NUMBER: IT-005
DIVISION: NET Services
POLICY: NSU Network Connectivity Policy
ISSUED BY: Chief Information Officer

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

INTRODUCTION

NET Services provides a secure network for educational, research, instructional and administrative needs. An unsecured device connected to the NSU network can leave the network compromised and vulnerable to viruses, Trojans, denial of service attacks and other security attacks. Therefore, users who connect computers, servers or other devices to the NSU network must follow very specific standards and guidelines.

PURPOSE

The purpose of this policy is to define the standards and guidelines for connecting computers, servers, and other devices to the University's network. The standards are designed to minimize the potential exposure to NSU from damages that could result from computers and servers not properly configured or maintained.

TARGET AUDIENCE

The NSU Network Connectivity Policy applies to all university-owned computers and personally-owned or leased computers that connect to the NSU network .

POLICY

- The CIO and the Network Security Officer will maintain an up-to-date list of all servers connected to the network that includes machine name, IP address, DNS name, location, server administrator(s), purpose, operating system, and major software.
- NET Services will maintain an inventory of all devices, including peripherals attached to the network and their physical location on campus.
- All requests for personal computer network connections to the NSU network must be directed through the NSU Help Desk or Computer Services.
- All computers connected to the NSU Network must be checked for viruses by NET Services personnel, have anti-virus software installed, and be approved by the Network Security Officer.

- No servers will be allowed to connect to the NSU network without prior written approval of the CIO. Administrators of approved servers must complete the *Server Authorization Form* before network connections will be made live.
- Network infrastructure devices connecting to the network must have prior approval from the CIO and Network Security Officer. This includes wireless access points, hubs, switches, routers, etc.
- Relocation of all equipment connected to the NSU network must be requested through the NSU Help Desk and is managed by the Computer Services Department.