



OIT 62.009: Network Administration

Responsible Executive: Chief Information Officer (CIO)
Responsible Office: Office of Information Technology
Related Policy: UP 60.201
Approved-On Date: February 13, 2006
Effective Date: February 13, 2006
Revision Date: December 17, 2009

Policy Statement

The Office of Information Technology (OIT) will operate and maintain a highly effective and efficient integrated University networking infrastructure with Internet access to meet the academic, research, and administrative needs of Norfolk State University.

Purpose

The purpose of this policy is to identify the circumstances when and how individual and/or department-level networking devices may be connected to integrated network operated and maintained by OIT.

Procedures

OIT operates and maintains local and wide area networks which are integrated and have been designed to serve all the computer systems installed at the University. The networking service that OIT provides is defined as “beginning at the jack on the wall” and ending at the Internet Gateway router or an internal host system. The service is defined in this manner to ensure that any properly formed packet sent from the attached computer through NSU’s network will be delivered to its destination, and vice versa.

Standards for the architecture and implementation of the campus network include specific topology; wiring; interconnection electronics, including many wireless access devices; and specific network technologies that are needed across the campus. Although OIT is responsible for installation and maintenance of this infrastructure, several departments have technical staff to assist in identifying new network requirements for expansion. In all cases, it is required that all installations follow the standards established by OIT for the campus network, including documentation and registration of connections. This is vital for OIT to properly maintain the campus networks and resolve any transmission or data communications issues which may arise.

Attaching Ancillary Equipment to the OIT-managed University Network

Network related issues are complex and require high levels of technical expertise to diagnose. In order to eliminate incompatibilities with different types of networking devices, OIT has identified specific network technologies and practices that are known to be reliable. OIT has implemented sound and widely accepted physical infrastructure requirements for routers, switches, wireless access points, and cabling. These strategies enable OIT to trace problems quickly and support a very large and ever expanding network with limited resources.

Because of the OIT operational requirements, personnel who are not assigned to OIT cannot connect ancillary devices, i.e. routers, hubs or switches, wireless access points, firewalls, network diagnostic equipment, or other networked devices – unless they have received proper authorization from OIT. Requests to attached devices to the network must be sent electronically to clientservices@nsu.edu. Any such requests received will be forwarded to the OIT Networks Technical Support Group where they can be thoroughly evaluated and the requestor may expect to receive a timely response from a qualified OIT network engineer.

Private Networks That Attach to the Campus Infrastructure

The creation of private networks that attach to the campus network greatly increases the difficulty in maintaining reliable network communications. In order to support the institution's networking requirements in an effective manner, OIT must put clearly defined limitations on its responsibility to support such attachments.

A few departments have chosen to install, operate, and maintain private networks without significant collaboration between the department's computer specialists and OIT. When departments do request that their networks be attached to the campus network, OIT offers alternatives:

- 1) OIT will coordinate with departmental staffs that have "private networks" to bring the local network infrastructure into compliance with current OIT infrastructure standards. This is the recommended strategy as OIT's engineering professionals will be able to maintain that infrastructure in the same way as the rest of the campus network. Once the infrastructure design is accepted and documented, attachment to the campus network can be accommodated and fully supported by the OIT networks technical support group.

- 2) If a department cannot rework their private network infrastructure to conform to OIT's networking guidance, OIT will have limited support for "the attachment of this private network" to the campus network. In particular, OIT can only warrant at best that network connectivity will be functional to the point where a private network attaches to the OIT supported Norfolk State University network.

Departments and activities that operate unsupported private networks must understand and agree to enforce University Policy 60.201: Acceptable Use of Technological Resources and any failure to enforce this policy could result in their connection to the University's OIT managed network being deactivated.

All Internet Protocol (IP) addresses used on any departmental private network will be assigned by OIT. Internet Domain Name Service for the private network will be coordinated with OIT.

Only those protocols supported by OIT will be routed from the private network. It is the private network operator's responsibility to support the communications services within that network for all computers attached to it. OIT requires that there be a designated technical contact for all private networks.

To request this service, the private network operator may either send an email to clientservices@nsu.edu or contact the OIT lead network engineer directly. OIT will do its best to ensure compatibility with the private networks.

OIT-Managed Campus Networks Change Management

Network configurations are managed through the OIT Change Management process. All modifications are presented to the Change Management committee before being implemented. All changes are discussed to determine the impact on the user community. All network configuration changes are scheduled at times that have minimal impact on the University's users and systems. OIT Policy 62.006: Information Systems Change Management is relevant.

Significant reconfigurations or upgrades to the network usually require separate technical meetings in addition to that performed in regularly scheduled Weekly OIT Change Management meetings. Technical committee meeting will include technical and or engineering representatives from all areas impacted by the change. The technical review committee will advise the Change Management team with pre and post configuration documentation on the most effective solution with least impact to University systems, users, and the network. The recommendations from the technical review committee will be reviewed by Change Management to be approved and scheduled.

All network systems and equipment affected by any network change will have their configurations backed up and saved. The configurations will be securely saved on OIT servers, on the network administrator workstation, and on USB removable drives or similar peripheral storage devices. The copies stored on OIT network servers are regularly backed up to magnetic tape media and then moved off-site. (Additional information is found in OIT Policy 62.002: Data Center Tape Backup Processes.) In this way, OIT can ensure all steps have been taken to retrieve configuration data in the event of catastrophic failure to any network systems.