

Effective Date: 8/1/2005

NORTH CAROLINA CENTRAL UNIVERSITY



1801 Fayetteville Street
Durham, NC 27707

Information Technology Services

New School of
Education
712 Cecil Street, 3rd.
Floor
Durham, NC 27707
(919)-530-7676

www.nccu.edu/helpdesk

Updated: August 2005

Wireless & Network Security Policy

Supersedes Policy Dated: New Policy

Approved: by the Board of Trustees on February 15, 2006.

Purpose of Policy:

This Policy has been developed to ensure that North Carolina Central University (NCCU) community has a secure and reliable network with access and the performance needed to carry out the goals of the university as well as meet the needs of its constituents. This policy will insure that Internet access to NCCU computing resources of the university and access to Internet resources are available to help fulfill the University's primary missions of instruction, research, and public service. This policy is intended to protect the integrity of the University network and to lower the risks and losses associated with security threats to the University network and computer systems that are part of NCCU computing environment.

NCCU Information Technology Services (ITS) provides wired (network jacks in residential Halls, classrooms, faculty and staff offices and wireless access to computing and information resources for students, faculty, and staff, within institutional priorities and financial capabilities.

NCCU Information Technology Services (ITS) also provides wireless networks operate on a shared and finite airspace spectrum. Information Technology Services (ITS) will regulate this airspace to ensure its fair and efficient allocation and to prevent collision, interference and failure.

Accidental or intentional disruption of a wireless network will deprive others of access to important University resources. Persons using wireless devices to connect to the University network must comply with all policies set in place by ITS, including the use of Cisco Clean Access Agent for the purpose of network authentication, Symantec antivirus software and Windows updates.

NCCU Information Technology Services (ITS) will approach the shared use of the wireless radio frequency in the same way that it manages the shared use of the wired network. Users may not provide network services that will interfere with the University network. ITS reserves the right to restrict the use of wireless devices on campus.

Policy:

This policy will:

- Provide a reliable network and Internet connection to conduct the University's business;
- Provide authorized access to institutional, research or personal data and information on the University network; and
- Protect computer system and network integrity at NCCU, and specifically, to protect University computing resources from:
 - Unauthorized access to University resources and/or information
 - Unintended and/or unauthorized disclosure of University information
 - "Denial of Service" attacks.

Threats NCCU's Network

The University network is subject to many risks. The risk of a "Denial of Service" (DOS) attacks from the Internet have occurred to many universities and corporations the past, and will most likely be attempted again in the future against University systems.

Risks to our academic mission are most apparent. The loss or corruption of data or unauthorized disclosure of information on research and instructional computers, student records, financial systems, or any other aspect of University operations is unacceptable. The University also has a legal responsibility to secure its computers and networks from misuse. This policy allows the University to handle network security responsibly.

The University considers any violation of Policy "Responsible Use of University Computing and Electronic Communication Resources," to be a serious offense and reserves the right to test and monitor security, including copying and examining any files or information resident on University computer systems allegedly related to unacceptable use. It is the responsibility of the Office for Information and Technology Services (ITS) to take the necessary steps to provide a reliable network.

This Policy applies to any existing or future connection(s) to the University's data network.

Addressing and Domain Services

1. Individuals, academic colleges/departments, or administrative departments at NCCU may not create or support an Internet domain hosted from the University's network without prior approval of the ITS.
2. ITS administers the NCCU IP address and the nccu.edu domain. ITS also manages any additional domains that support the mission of the University.
3. Technological changes and other factors may require a reconfiguration of the network resulting in a change to the network addresses assigned to University computers. ITS will give prior notice to affected users before making any changes.

Network Connections, wired and wireless

1. No NCCU departments, faculty, staff, or students may connect, or contract with an outside vendor to connect, any network device, i.e., wireless access points, hubs, switches or routers, or system to the University's data networks without the prior review and approval of ITS.
2. Colleges or departments that wish to provide Internet or other network access to individuals or networks not directly affiliated with the University must obtain prior approval from ITS.
3. Accidental or intentional disruption of the network will deprive others of access to important University resources. Persons using any device to connect to the University network must comply with all policies set in place by ITS, including the use of Cisco Clean Access Agent for the purpose of network authentication, Symantec antivirus software and Windows updates.
4. Physical access to University networking equipment (routers, switches, hubs, etc.) is not permitted without the prior approval of ITS.
5. ITS provides a general method for network authentication to University systems, using Cisco Clean Access Agent.

External Services and Requests

1. ITS will take action to prevent source network address forgery (spoofing) of internal network addresses from the Internet. ITS will also take action to protect external Internet sites from source address forgery from the University's network.

2. The University's external Internet firewall policy is to deny all external Internet traffic to the University's network unless explicitly permitted. Access and service restrictions may be enforced by IP address and/or port number. Proxy services may be used in conjunction with the firewall to restrict usage to authenticated individuals. This policy is designed to protect University network users from attacks launched from the Internet.

3. The University's internal Internet firewall policy is to deny specific internal IP traffic outbound to the Internet unless explicitly permitted. This policy is designed to protect others on the Internet from attacks launched from the University's network.
4. Some network services through standard ports are supported. However, services may be restricted to a limited number of subnets or hosts. For example, electronic mail (e.g., SMTP, Port 25) may be sent and received only by authorized mail servers on campus. User access to the mail accounts (e.g., POP3, Port 110 and IMAP, Port 143) on these servers will be permitted from off-campus through the firewall.
5. Most network services through non-standard ports are not supported. Services through non-standard ports may be restricted to a limited number of subnets or hosts. For example, WWW access via the standard HTTP port (Port 80) will be permitted, but via some other arbitrary port number may not be permitted.
6. Limited encrypted tunnels for passing through the firewall to internal resources, such as X-Windows, is permitted with the prior approval of ITS. The recommended method is to use Secure Shell (SSH). IP Multicast tunneling is not permitted.

Network Security

1. In collaboration with academic and administrative departments, ITS shall identify the appropriate network security level for University systems. These levels are, from highest to lowest: Mission-critical, Important, Normal and Low. Efforts shall be made to protect University computer systems and review it periodically.
2. In coordination with administrative departments and law enforcement, ITS will investigate, or cause to be investigated, any unauthorized access to University computer systems.
3. Systems on the network must have adequate security installed and maintained. All systems connecting to the University network must be configured and maintained in such a manner as to prohibit unauthorized access or misuse. For example, a guest account must have a secure password.
4. It is the responsibility of all NCCU network users to report security problems to the appropriate system administrators or ITS for investigation.
5. Network usage judged appropriate by the University is permitted. Some activities deemed inappropriate include, but are not limited to:
 - o Establishing unauthorized network devices, including a router, gateway, or remote dial-in access server; or a computer set up to act like such a device.
 - o Engaging in network packet sniffing or snooping.
 - o Operating network servers of any sort in violation of ITS guidelines.
 - o Setting up a system to appear like another authorized system on the network.
 - o Other unauthorized uses prohibited by this Policy or other ITS organization policies.

Wireless Networks

The University reserves the rights to limit, restrict, or extend access to the wireless airspace on campus. Any person operating a wireless device that interferes with existing central network services or overload the network, will be notified and steps will be taken to protect the overall University network. This may include disconnecting the offending computer device from the network until the problem is resolved. If the condition is an imminent hazard to the University network or disrupts the activities of others, then the offending computer may be disconnected without prior notice.

Any person attaching a wireless device to the University network is responsible for the security of the computer device and for any intentional or unintentional activities from or to the network pathway that the device is using. Users and system administrators must all guard against abuses that disrupt or threaten the viability of all systems. Access to information resources without proper authorization from the data owner, unauthorized use of University computing facilities, and intentional corruption or misuse of information resources are direct violations

North Carolina Central University's standards for conduct.

Guidelines:

Wireless Spectrum

- NCCU regulates and manages all unlicensed radio frequencies on campus. Wireless equipment installed by ITS uses either the FCC unlicensed 2.4 GHz Industrial/Scientific/Medical (ISM) band or the FCC 5.0 GHz Unlicensed National Information Infrastructure (U-NII) band.

- Wireless equipment transmissions within the 2.4 GHz and 5.0 GHz bands conform to current IEEE 802.11 wireless LAN specifications.
- Other wireless devices that also use the above mentioned frequency bands, including but not limited to wireless LAN devices, cordless telephones, cameras, and audio speakers, will cause interference with ITS-installed devices. As such, use of these devices is prohibited on the University campus.
- ITS may restrict the use of any potentially interfering wireless radio device in university-owned buildings and all outdoor spaces on the NCCU campus.
- Faculty who believe they have special wireless needs should contact ITS.

Wireless Network Operation and Security

- The enterprise wireless infrastructure is managed campus-wide by ITS.
- ITS will provide spectrum tuning, and general device management per access area according to wireless access device management standards.
- Wireless networks will be segmented and treated as a “foreign/un-trusted network” from a security standpoint. A firewall, router/switch VLAN technology, or similar technology will be employed to provide this segmentation.
- Wireless users must be authenticated with unique user credentials.
- Only authorized access points will be permitted. Unauthorized access points will be disabled.
- Unauthorized traffic interception and/or bridging between the wired and wireless network is prohibited.
- Applications supported over the wireless network will be limited, as long as this is necessary to provide an acceptable quality of service for all users.
- No wireless spectrum interference or disruption of other authorized communications is permitted

Security

ITS will maintain the highest security available for the device installed. Security of the wireless network has many facets. Physical security of the wireless devices will be maintained whenever possible. In common areas, appropriate precautions will be taken to protect the Access Point from theft or access to the data port. Hardware MAC addresses will be maintained in a DHCP server. Access to the wireless network will only be allowed from valid entries in the DHCP server.

Violations:

ITS will enforce the *Wireless Communications Policy* and establish standards, procedures, and protocols in support of the policy.

Any violation of this policy by faculty and staff is “misconduct”. Any violation of this policy by students is subject to the Student Code of Conduct in the student handbook. Violations of law may also be referred for criminal or civil prosecution.

ITS has the authority to disconnect network service or modify/enhance network security without notification in the event of law violation, systems compromise.

Monitoring and Auditing

1. ITS maintains traffic logs of the firewall for security auditing purposes.
2. To safeguard the integrity of the University's computing and electronic communication resources, and to minimize the risks to both those resources and the end users of those resources, ITS will monitor data traffic to detect anomalous network activity and will access, retrieve, read, and/or disclose data communications when there is reasonable cause to suspect a violation of applicable University policy or criminal law, or when monitoring is otherwise required by law.
3. With the permission of the system administrator or his or her superior, ITS may perform a security audit of any computer system attached to the University's network. ITS will provide a report after the audit is completed.

Enforcement

1. Any device found to be in violation of this Policy, or found to be causing problems that may impair or disable the network in any way, is subject to immediate disconnection from the University's network. The Data Network Services Department or other IT departments may require specific security improvements where potential security problems are identified.
2. Attempting to circumvent security or administrative access controls for information resources is a violation of this Policy. Assisting someone else or requesting someone else to circumvent security or administrative access controls is also a violation of this Policy.

Policy Management

The Chief Information Officer (CIO) is authorized to appoint an Information Technology Security Officer who shall be responsible for the enforcement, interpretation, and administration of this Policy.