



THE UNIVERSITY OF NORTH CAROLINA
ASHEVILLE

Policies and Procedures

Policy #: 78
Page: 1 of 2
Contact Dept: ITS
Phone: 251-6445

Title: Network Security

Purpose: The purpose of this policy is to establish a framework for the management and administration of security of the university data network.

Scope: This policy applies to all existing and future connections (wired and wireless) to the university data network by students, employees, guests, and academic and administrative departments.

Policy: Information Technology Services (ITS) will protect the integrity of the university network by mitigating the risks and losses associated with security threats to the university network and information systems.

Information Technology Services is charged with:

1. Providing a reliable network and Internet connection to conduct the university's business.
2. Providing only authorized access to institutional, research or personal data and information on the university network.
3. Protecting computer system and network integrity at UNC Asheville and specifically:
 - a. Protecting university computing resources from unauthorized access.
 - b. Protecting university information from unintended and/or unauthorized disclosure.
 - c. Monitoring the university network for devices and users in violation of this policy.

To accomplish these charges

1. Information Technology Services will develop and maintain guidelines for network connections and for configuration of network-connected devices. These guidelines are found in the document 'Networking Procedures/Guidelines' in the ITS documentation library.
2. Information Technology Services has the authority to fully enforce adherence to its network security guidelines.
3. Information Technology Services will proactively monitor/scan for security weaknesses in the network or any equipment connected to the network and will provide an audit report to the equipment owner after the scan/audit is completed.

4. The Information Security Officer(s) in Information Technology Services along with the Chief Information Officer (CIO) are responsible for the interpretation, administration, and enforcement of this policy.

Information Technology has the authority to disconnect from the network any device which may impair or disable the network; compromise the integrity of other network-connected devices; threaten the security of university data stored on the network; or be used for activities which violate university policies or state and federal statutes.

Additionally, a violation of this policy may be regarded as a violation of other university policies governing the conduct of university community members, and may therefore result in sanctions and disciplinary actions under the provisions of those policies.

Approved on: 10/28/08
Next review: 10/28/10