NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

SEC.VII — NETWORK 1.0

NETWORK USAGE

University Policy

I. Purpose

This policy provides guidelines for users connecting to the North Carolina A&T State University network. This policy applies to all University networked devices, ranging from multi-user systems to single user personal computers and mobile devices; included under this policy are networked printers, mini-hubs, routers, switches, and any other network communication devices, which are connected to the University's network. This policy protects the operational stability, performance and security of all devices connected to the network and promotes a safe network environment for education, research and other institutional priorities.

II. Scope

This policy defines the rules, guidelines and standards that users of the University's network must adhere to when using any of the networking resources and actions that will be taken when any of the rules, guidelines or standards is violated.

III. Policy Statement

The University's network includes all physical copper and fiber data cabling at the University, Virtual Private Network (VPN) connections, and all remote locations which allow devices to be connected directly to the University's network via wired or wireless means.

The networking environment and activity will be monitored and analyzed to ensure usage of the university's network is consistent with this policy. Authorization to connect from Networking and Communication Services requires that users agree to adhere to this Network Usage Policy. A&T reserves the right to limit, restrict, or extend computing privileges and access to its resources.

The University's network is not a public forum and shall not be used in such a manner. It is intended only for use by A&T employees, students, and other authorized users.

Network resources can provide access to resources both on and off campus. Such open access is a privilege, and requires that individual users act in a responsible and acceptable manner. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. Acceptable use demonstrates respect for intellectual property, truth in communication, ownership of data, system security mechanisms, and individuals' right to privacy and freedom from intimidation, unlawful harassment, and unwarranted annoyance. The university considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to test and monitor security, and copy and examines any files or information resident on A&T's systems allegedly related to unacceptable use.

A&T's Networking and Communication Services should be notified about violations of computer laws and policies, as well as about potential loopholes in the security of its computer systems and network. The user community is expected to cooperate with Networking and Communication Services in its operation of computer systems and networks as well as in the investigation of misuse or abuse.

IV. Guidelines

A. Acceptable Devices

Any computer, peripheral or network capable device connected to NC A&T's network must belong to an individual who is a current University employee, student or a guest of the University. Devices connected to the network shall be in good working order and be designed or configured not to interfere with other devices connected to the network or the network operations of the University. Devices connected to the network must be used for an activity related to University business and adhere to the University’s connectivity and security requirements.

Any new device requesting network access will be monitored and compliance ensured before devices are allowed to connect. Workstations, laptops, mobile devices, servers and any other user devices must be configured to ensure they meet network configuration requirements. Devices that don’t meet the university’s configuration requirements should not be connected to the network.

Hubs, switches, routers and wireless devices should never be connected to the University data network without prior approval from Network and Communication Services. These devices when configured incorrectly have the potential to disrupt the network availability or stability.

All networking equipment connected to the University network must first be registered and approved by Networking and Communication Services.

All wireless devices connecting to the University network must be registered and/or properly authenticated. Devices connected to the network cannot interfere with the operation of the University network.

Any networked devices or services that are detected and verified to degrade the quality of service on the network will result in termination of network service of that device until the cause of the problem is corrected.

B. Responsible Parties

The Owner or Responsible Party (RP) of a device connected to the campus network must have a valid University email account and phone number in order to facilitate contact if there is a problem with the device. The Owner or RP is responsible for the use or misuse of their device attached to University’s network. A&T’s Networking and Communication Services reserves the right to restrict access to devices which are connected to the network through a MAC address or IP address blocking / redirection.

C. Building Wiring Closets and Backbone Network

Campus building wiring closets and network/telecommunication equipment cabinets are the sole responsibility of A&T’s Networking and Communications Services and should only be accessed by DoIT staff and other authorized University personnel.

Network/telecommunications equipment housed in shared mechanical and/or janitorial rooms shall only be accessed by authorized DoIT staff. Campus core, distribution and access layer equipment (switches, routers and wireless access points responsible for building-to-building communication) are only to be accessed and configured by authorized DoIT staff.

D. Security

Security measures must be taken to ensure that devices connected to the University's network are not vulnerable to compromise. Recommended actions for devices connected to the University's network include: keeping software current; patching operating systems; current anti-virus software and virus definitions; secure passwords; personal firewalls; and intrusion detection software. Compromised or problem hosts connected to the University's network will be blocked until they are repaired and evaluated.

E. Unacceptable Activities

DoIT will not support or condone the activities listed below:

- Activities which excessively consume network resources;
- Activities which violate this and/or other University Policies;
- Activities which violate municipal, state and/or federal laws;

Unacceptable activities include, but are not limited to:

- Providing services which interfere with the legitimate function of other devices connected to the University's network (examples include DHCP servers, devices running routing protocols, remote access servers consuming addresses which have not been registered with DoIT);
- Interfering with the supervisory or accounting functions of any system owned or managed by the University,
- Unauthorized commercial activities;
- The sending of SPAM (Unsolicited Bulk and / or Commercial Email);
- Open email relays;
- Denial of service attacks;
- Hacking / cracking or any form of data intrusion / attack;
- Probing, scanning or other activities done to learn about devices connected to the University's network, whether such activity is innocent or malicious in nature.

(Exceptions are made for system administrators and DoIT staff performing security scans on systems they manage in the course of their job duties);

- Packet and content sniffing;
- Unauthorized access to hosts connected to the University's network or other networks;
- Illegal distribution of copyrighted material;
- "Stealing" or "borrowing" IP addresses;
- Any form of harassment in violation of federal or state law
- Activity such as threatening the safety of individual(s) and/or property, intimidating or bullying individual(s), defamation of individual(s), and violation of student and/or employee policies
- Intentionally disrupting any business, academic or research activities of the University conducted via the University's network

V. ENFORCEMENT

University sanctions for a user cited for policy violations include but are not limited to one or more of the following:

- Suspension of information system(s) privileges; in order to reduce the number of credentials used to access University resources, single sign-on/reduced sign-on identity management solutions are enabling users to access multiple resources with the same credentials. Suspended access will impact a student's ability to complete academic requirements and an employee's ability to perform his or her job duties.
- Misconduct review.
- Termination or discharge of employment.
- Student dismissal.
- Breach of contract/agreement filed against guests.

For University students and employees, sanctions will be administered in accordance with governance from the University's policies, the student handbook, the faculty handbook, policies of Human Resources, and the Office of State Human Resources procedures.

Date Policy is Effective: Upon approval

Approved by the Board of Trustees

First approved: November 22, 2013
Revised: