	NORTH CAROLINA A&T STATE UNIVERSITY **CHAPTER 700 – INFORMATION TECHNOLOGY** **UNIVERSITY STANDARD US706,** **TELECOMMUNICATIONS ROOMS AND ENCLOSURES**

SECTION 706.1 STANDARD STATEMENT

Telecommunications Rooms and Enclosures are secure areas as described in the North Carolina A&T State University's (N.C. A&T or University) Policy 701, Information Security (ISP) and University Standard US701, Access Control (ACS), and fall under the information resource trusteeship of the vice chancellors for Business and Finance and Information Technology Services (ITS). The responsibility for the security and integrity of the University's Telecommunications Rooms and Enclosures is shared between ITS and Business and Finance.

Management and oversight of N.C. A&T's networks is the responsibility of ITS and is delegated to the Department of Network and System Administration.

SECTION 706.2 PURPOSE

This document defines the standards, practices, and procedures to manage and secure all Telecommunications Rooms and Enclosures owned or operated by N.C. A&T, regardless of location or specific purpose. This includes requirements to manage physical security of all telecommunications equipment housed within these locations. This standard is an extension of the ISP, University Policy 702, Acceptable Use (AUP), and the ACS, and provides additional technical specifications. All requirements and sanctions of these policies and the ACS apply to this standard. This standard also outlines requirements for compliance with the North Carolina Fire Code as required by the Greensboro Fire Department.

SECTION 706.3 SCOPE

This document includes requirements for the construction of Telecommunications Rooms and Enclosures as well as standards and practices for the recurring maintenance of existing Telecommunications Rooms and Enclosures. It applies to all Telecommunications Rooms and Enclosures that house telecommunications equipment that are owned or managed by N.C. A&T without regard to the location or specific purpose. In addition to management and security items, this document includes guidelines to ensure telecommunications resiliency and support business continuity efforts.

SECTION 706.4 DEFINITIONS

"ACS" refers to N.C. A&T's standard on access control, University Standard US701, Access Control.

"AUP" refers to N.C. A&T's policy on acceptable use. University Policy US702, Acceptable Use.

"Dedicated Telecommunications Room" means a Telecommunications Room dedicated to housing telecommunications equipment and not used for other purposes.

"Enclosure" means a rack, cabinet or other container designed to house telecommunications equipment or cabling. This term includes Fiber Enclosures and Stand-Alone Telecommunications cabinets.

"Fiber Enclosure" means an enclosure, such as a cabinet, pedestal, handhole, or other utility enclosure intended for the housing, termination, or cross connection of fiber optic cabling.

"Free-Standing Telecommunications Equipment" means Telecommunications equipment, such as wireless access points, which are not housed in a Telecommunications Room or Enclosure.

"ISP" refers to N.C. A&T's policy on information security, University Policy 701, Information Security.

"Network Administrator" means any individual whose duties include installation, management, maintenance, or configuration of telecommunications equipment, regardless of position title.

"Shared Telecommunications Room" means a Telecommunications Room that houses telecommunications equipment owned by NCA&T or others and is also used for additional purposes.

"Stand-Alone Telecommunications Cabinet" means a cabinet that houses telecommunications equipment that connects, constitutes, or otherwise establishes a N.C. A&T network but is not located in a specific Telecommunications Room.

"Telecommunications Room" means a room that houses telecommunications equipment that connects, constitutes, or otherwise establishes a N.C. A&T network, and includes Dedicated Telecommunications Rooms, Shared Telecommunications Rooms, and Enclosures unless otherwise stated.

SECTION 706.5 COMPLIANCE

Standards derived from the ISP are mandatory for all employees, students and affiliates. Failure to adhere to these standards may result in disciplinary action, up to and including dismissal, suspension or expulsion, or termination of privileges.

SECTION 706.6 RESPONSIBILITIES

Vice Chancellors of Business and Finance and Information Technology Services

The vice chancellors are responsible for implementing controls, as described in the ISP, AUP, ACS, and this standard, to mitigate the risks associated with access and maintenance of Telecommunications Rooms, Enclosures, and Free-Standing Telecommunications Equipment.

Associate Vice Chancellor for Facilities

The Associate Vice Chancellor (AVC) for Facilities is responsible for approving access to Telecommunications Rooms and Enclosures for staff members from Facilities, and for ensuring that Facilities staff comply with this standard.

Associate Vice Chancellor for Information Technology Services and Deputy Chief Information Officer

The AVC for ITS is responsible for approving access to Telecommunications Rooms and Enclosures for staff members from ITS and additional units, excluding Facilities and the University Police Department (UPD). The AVC is also responsible for ensuring that all ITS staff and others with delegated access comply with this standard.

Associate Vice Chancellor for Public Safety/Chief of Police

The AVC for Public Safety/Chief of Police is responsible for approving access to Telecommunications Rooms and Enclosures for officers and staff members of UPD, and for ensuring that officers and staff members comply with this standard.

Director of Network and System Administration

The Director of Network and System Administration (DNSA) is responsible for managing Dedicated Telecommunications Rooms, Enclosures, Free-Standing Telecommunications Equipment, and the University's network. The DNSA is also responsible for ensuring that: (1) equipment is properly installed and secured; (2) temperature is monitored; (3) Dedicated Telecommunications Rooms and Enclosures remain locked; and (4) periodic inspections are performed. The DNSA shall ensure that procedures are documented and performed in compliance with this standard and shall maintain records of these actions in order to demonstrate compliance during security assessments or other reviews.

The DNSA shall ensure that any issues relating to the physical plant of Telecommunications Rooms and Enclosures are reported to Facilities in a timely manner and with the appropriate priority level based on the severity and impact of the issue. The DNSA shall also ensure the communication of this standard and responsibilities to ITS staff members.

Director of Facilities Operations

The Director of Facilities Operations (DFO) is responsible for addressing any issues related to the physical plant of Telecommunications Rooms and Enclosures in a manner consistent with the extent, priority, and impact of the issue as communicated by the DNSA. The DFO is also responsible for ensuring the communication of this standard and responsibilities to Facilities staff members.

Network Administrators

Network administrators are responsible for proper installation, configuration, and securing of telecommunications equipment. Network administrators must also adhere to all procedures and tasks and document their actions.

Other

These standards apply to any other person granted or having physical access to Telecommunications Rooms or Enclosures.

SECTION 706.8 REQUIREMENTS

Section 706.8.1 Access Control

All requirements of access control and physical security specified in these documents apply to all Telecommunications Rooms. All access control authorization shall be guided by the ACS.

The associate vice chancellors for Facilities and ITS shall authorize access to Telecommunications Rooms for their respective staff members.

The Chief of Police shall authorize access to Telecommunications Rooms for UPD officers and staff members.

The Associate Vice Chancellor for ITS shall authorize access to Telecommunications Rooms for additional staff as needed to meet academic, research, or business needs.

Section 706.8.2 Operation

Dedicated Telecommunications Rooms shall be used whenever one is available for use. Dedicated Telecommunications Rooms shall not be used for storing other equipment or supplies.

New construction projects shall include Dedicated Telecommunications Rooms compliant with the requirements of this standard. Renovations shall include Dedicated Telecommunications Rooms as appropriate.

When dedicated rooms are unavailable, Shared Telecommunications Rooms may be used for additional purposes. In these cases, all the remaining requirements of this standard shall apply.

Buildings with multiple floors shall have at least one Telecommunications Room on each floor. Rooms shall be located so that the maximum length of horizontal cabling is less than 300 feet.

The University has installed Stand-Alone Telecommunications Cabinets in locations where dedicated or shared rooms were not originally available. The use of Stand-Alone Cabinets is prohibited unless Dedicated Telecommunications Rooms or Shared Telecommunications Rooms are unavailable.

Generally, Telecommunications Rooms shall have no windows. When a Telecommunications Room has windows, whether facing the exterior or interior of the building, the windows shall be reinforced and secured to prevent access by unauthorized persons.

Telecommunications equipment, including wall-mounted equipment in shared rooms, shall be accessible and shall not be obstructed by other equipment or supplies. A clear space with a minimum width of three (3) feet shall be maintained around all telecommunications equipment cabinets or racks. A clear path with a minimum width of three (3) feet shall be maintained from the equipment rack to the nearest door, and any other door to the closest building exit.

All items stored in a Shared Telecommunications Room shall be kept orderly, tidy, and generally organized. Generally, items shall be stored on shelving units. Shelving units shall be securely attached to walls to provide the structural integrity necessary to prevent the stored items from tipping or falling onto telecommunications equipment.

Shelving units shall not be erected in places where a failure of the unit would cause items to fall onto telecommunications equipment, cabinets, or racks.

Section 706.8.3 Environmental Control and Safety

Generally, Dedicated and Shared Telecommunications Rooms shall be configured with a stand-alone air conditioning unit.

Temperature in each Dedicated or Shared Telecommunications Rooms shall be maintained at or below 80 degrees Fahrenheit.

Rooms that contain Stand-Alone Telecommunications Cabinets shall be maintained at or below 80 degrees Fahrenheit.

Humidity in each Dedicated or Shared Telecommunications Rooms shall be maintained at a relative humidity between 40% and 60%.

Rooms that contain Stand-Alone Telecommunications Cabinets shall be maintained at a relative humidity between 40% and 60%.

Telecommunications Rooms shall employ a monitoring system to alert staff when the temperature of any room exceeds the required levels.

Telecommunications Rooms shall be maintained free from rust, water, dirt, trash, debris, and other contaminants.

Dedicated Telecommunications Rooms shall be free of all flammable materials not specifically intended for the connection, constitution, or establishment of a N.C. A&T telecommunications network.

Shared Telecommunications Rooms shall have no flammable item, material, or substance placed, stored, or located within ten (10) feet of network equipment. Examples include, but are not limited to, paper, paints, and solvents.

Telecommunications Rooms shall be equipped with properly rated fire-retardant ceiling tiles. Tiles shall be free from cracks, holes, and other damage, except where necessary to facilitate proper wiring.

All breaks, holes, or penetrations in ceiling tiles shall be filled with properly installed fire barrier material rated for two (2) hours or longer of fire resistance, in accordance with the North Carolina Fire Code.

Telecommunications Rooms shall be equipped with a fire extinguisher carrying a class "C" rating specifically intended for electrical fires. Fire extinguishers shall be within one hundred and fifty (150) feet of the entrance and maintained in proper working order.

Dedicated Telecommunications Rooms shall have no water source within the room that is not solely intended for fire suppression.

Shared Telecommunications Rooms and Stand-Alone Telecommunications Cabinets shall have no water source within ten (10) feet horizontally of network equipment and shall have no water sources directly overhead that are not solely intended for fire suppression.

A drip pan shall be properly installed and maintained below all water supplies, drains, or condensation pipes running over the top of network equipment.

Shared Telecommunications Rooms shall not have any equipment stored within ten (10) feet of network equipment that utilizes or contains liquid when stored (e.g., power cleaners that contain liquid when stored).

Shared Telecommunications Rooms may contain equipment that utilizes liquid during operation but does not contain liquid when stored (e.g., a mop bucket that is empty when stored).

Shared Telecommunications Rooms may contain electrically powered maintenance equipment if storage of the electrical equipment complies with this standard. Electrical cords shall be properly wrapped and stored to avoid tripping hazards, and properly maintained to prevent fire hazards.

Telecommunications equipment shall be installed in equipment cabinets or racks with proper mounting hardware in order to ensure a safe and stable installation.

Telecommunications Rooms shall be equipped with signage that clearly designates the space as an ITS Telecommunications Room and prohibits unauthorized access.

Telecommunications rooms shall be equipped with a current and accurate building evacuation plan.

Section 706.8.4 Security

Dedicated Telecommunications Rooms, Shared Telecommunications Rooms~~,~~ and Stand-Alone Enclosures shall be locked at all times unless a staff member with authorized access is working in the immediate vicinity. Authorized staff shall monitor others who require access to these locations.

Telecommunications equipment shall be installed in cabinets in shared equipment rooms. Stand-Alone Telecommunications Cabinets shall be fully enclosed and configured with properly installed front, back, top, bottom, and side panels. Panels shall remain locked except during installation, removal, or maintenance activities.

Employees or contractors shall provide ITS with timely notification of any issues that lack compliance with this standard or compromise the safety or security of a Telecommunications Room or Stand-Alone Telecommunications Cabinet.

Section 706.8.5 Power and Cabling

All Telecommunications Cabinets shall be equipped with one dedicated four receptacle NEMA5-20R 20A/120 electrical outlet fed from the building circuit panel and terminated inside each cabinet, rack, or enclosure.

Telecommunications Rooms shall be equipped with an uninterruptible power supply (UPS) capable of sustaining the telecommunications equipment for one (1) hour or longer.

Telecommunications Rooms' wiring shall be kept orderly, tidy, and properly dressed following best practices as outlined in the Building Industry Consulting Service International Standard for Installing Commercial Building Telecommunications Cabling.

Telecommunications Rooms shall be equipped with a grounding wrist strap. The wrist strap shall be used whenever staff members install, remove, or perform any maintenance on equipment.

Telecommunications equipment shall utilize properly grounded electrical outlets connecting all equipment power to the building power ground or house ground.

Metal Telecommunications Cabinets or racks that reside on top of carpet shall be properly grounded by connecting the metal cabinet or rack directly to the building power or house ground.

Stand-Alone Telecommunications Cabinets shall have power receptacles terminated inside the cabinet with flexible metal conduit connecting the cable to the nearest wall.

Section 706.8.6 Inspection

ITS shall inspect each Telecommunications Room and Stand-Alone Telecommunications Cabinet for compliance with this standard on a quarterly basis. Additional inspections may be conducted to meet other requirements such as compliance with the North Carolina Fire or Electrical Codes. Inspection records or copies shall be shared with ITS. ITS shall maintain records for at least two (2) fiscal years.

SECTION 706.9 AUTHORIZATION OF ACCESS

Access to Telecommunications Rooms and Enclosures shall be based on Sections 2 and 8 of the ACS. Only staff members with specific duties in Telecommunications Rooms or Enclosures shall be granted access. The AVCs for Facilities and ITS and the Chief of Police may grant access to classes of employees or to individual staff members on their respective staffs. The AVC for ITS may grant access to classes of employees or to individual staff members in additional units.

Access to Telecommunications Rooms or Enclosures shall be based on the need to install, remove, or maintain telecommunications or other equipment, such as air conditioners, to access supplies stored within the room, or the need for human safety and security.

Access to Shared Telecommunications Rooms for staff in other units will be evaluated based on the risk of access and the business need for access. The unit requesting access shall provide documentation of the business need. The storage of a unit's items in a shared network room does not predicate access authorization. Upon approval of access, the respective unit shall accept all risk associated with said access on behalf of the University. Furthermore, said unit shall bear all responsibility for said access and shall be responsible for all costs resulting from any damage or penalties resulting from the use of said access.

SECTION 706.10 EXCEPTIONS

This standard does not apply to Telecommunications Rooms or Enclosures that are owned and managed by other organizations that use those rooms or enclosures to provide services to N.C. A&T, such as third-party telecommunications providers. Departments that subscribe to services that are owned and managed by other organizations shall obtain evidence of appropriate management and security controls from the service provider.

This document does not apply to network equipment in a laboratory environment used for instruction or research that is segmented or physically separated from the rest of the N.C. A&T network. Segmentation of that equipment shall include limitations on access from said equipment

to other parts of the University network and the Internet. These limitations shall be developed in cooperation with and approved by ITS before the equipment is connected to any N.C. A&T network. Physically separated equipment shall remain physically separate and shall not be connected to any N.C. A&T network without ITS approval.

ITS may approve exceptions to any portion of this standard that conflicts with the institutional purpose of specific telecommunications equipment, such as testing of new types of equipment or the facilitation of research. All remaining portions shall apply. When exceptions are approved, the Network Administrator shall work with the functional unit and ITS to implement alternative security measures to protect the Telecommunications Room, Enclosure or equipment, the University's network, and other University information resources. ITS shall approve the configuration, including all such alternative measures, prior to connecting any telecommunications equipment to a N.C. A&T telecommunications network.

Exceptions to this standard shall undergo a formal risk assessment and must be approved in writing by the Vice Chancellor for Information Technology or the VC's designee.

STANDARD HISTORY:

Eff. February 8, 2021

AUTHORITY: Chancellor

STANDARD OWNER: Vice Chancellor for Information Technology

RESPONSIBLE OFFICE: Information Technology Services

RESOURCES:

UNC Policy 1400.1 Information Technology Governance
ISO 27002:2013 Code of Practice for Information Security Controls
N.C. A&T Policy 701, Information Security
N.C. A&T Policy 702, Acceptable Use
N.C. A&T Standard US701, Access Control
Building Industry Consulting Service International Standard for Installing Commercial Building Telecommunications Cabling