NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

SEC. VII – EQUIPMENT USE 4.0

ACCEPTABLE USE

UNIVERSITY POLICY

I. Purpose

This policy outlines the acceptable use of information resources at North Carolina Agricultural and Technical State University (N.C. A&T). Information resources are provided for university-related purposes and include all hardware, software and data owned or operated by the university regardless of form or location. Access to and use of information resources entails specific expectations and responsibilities for users and technical staff that are set forth in this policy.

II. Scope

This policy applies to all university information resources, regardless of form or location, and the hardware and software resources used to electronically store, process or transmit that information. This includes data processed or stored and applications used by the university in hosted environments in which the university does not operate the technology infrastructure. All N.C. A&T employees, students and affiliates (users) must adhere to this policy.

III. Definitions

A. Affiliate

An affiliate is an individual who requires access to information resources to work in conjunction with the university, but is not an N.C. A&T employee or student. Affiliates

may also be retired N.C. A&T employees who have been granted access to a defined set of information resources. Affiliates must have a sponsor who is an employee. Retired employees who are affiliates are sponsored by Human Resources.

B. Information Resources

Information resources are information owned or processed by the university, or related to the business of the university, regardless of form or location, and the hardware and software resources used to electronically store, process or transmit that information. Information resources expressly include data, software and physical assets.

C. University Data

University data are information resources that include information created, acquired, maintained, processed or transmitted by or on behalf of N.C. A&T, regardless of form or location, and utilized in the management and operation of educational, research or business activities.

D. University Network

The university's network includes all physical copper and fiber data cabling at the university, the network device infrastructure, Virtual Private Network (VPN) connections, and all remote locations that allow devices to be connected directly to the university's network via wired or wireless means. This includes networks at remote locations where the network is managed by the university.

IV. Policy and Procedure Statements

A. Requirements

N.C. A&T's information resources and a trusted and effective information technology environment are critical to support its mission of teaching, learning, discovery and community engagement, and to attain the university's goals and objectives. In furtherance of this mission, the university makes information resources available for a variety of purposes, including support of scholarship, research, instruction and campus life activities, to facilitate the operations of the university, and to provide access to university services.

Users are responsible for the proper use and protection of information resources and respecting the rights of other users. Access to information resources, including data, software, hardware and network resources owned by N.C. A&T, is a privilege that imposes specific responsibilities and obligations, and is granted to a user subject to federal and state regulations and university policies.

1. Operations and Maintenance

The normal operation and maintenance of the university's information resources require back up and caching of data and communications, the logging of activity, monitoring of general usage patterns and other such activities. N.C. A&T may, with or without further notice to users, take any other action it deems necessary to preserve, protect and promote the interests of the university. Such actions include, but are not limited to, those listed below and may occur at the institutional or local unit level pursuant to procedures promulgated from time to time under the Information Security Policy.

a. Monitoring – The university may intercept, access, scan, inspect, monitor, record, copy, store, use, disclose or sanitize the contents of any electronically stored data employing information resources or any communications or transmissions to or from information resources, whether via computer accounts, devices or other means.

b. Unauthorized Access – The university may block unauthorized access to, and unauthorized uses of, information resources.

2. General Use and Ownership

a. Acceptable Use – Acceptable use is always ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. Acceptable use demonstrates truth in communication, respect for intellectual property, ownership of data, system security mechanisms, and an individual's freedom from intimidation, unlawful harassment, and unwarranted annoyance.

b. Efficient Use of Resources – Information resources are finite and must be shared. The university retains the right to set priorities on the use of information resources, and to limit recreational or personal use when such use could reasonably be expected to cause direct or indirect strain on any information resources facilities; to interfere with scholarship, research, instruction or operations of the university; or to violate applicable policies or laws.

c. Ownership – All university data stored on electronic and computing devices remains the sole property of N.C. A&T unless ownership is assigned to another party by regulation, policy or contractual agreement. This applies to all devices whether owned or leased by the university, the employee or a third party. Users must ensure that confidential, sensitive and controlled data is accessed, used and protected in accordance with the Information Security Policy and related standards and procedures.

d. Incidental Use – Incidental personal use is permissible to the extent that it does not unreasonably interfere with the use of information resources by other users, or with the university's operation of information resources; interfere with the user's employment or other obligations to the university;

or violate any legal regulation and this or other applicable policy. Users are expressly forbidden to use university information resources for personal gain.

e. Expectation of Privacy – Users have no expectation of privacy in connection with the use of university information resources. The university may access and monitor its information resources for any purpose consistent with the university's duties and/or mission without notice. Users should have no expectation of privacy regarding any university data residing on personally-owned devices, regardless of the reasons that the data was placed on the personal device.

f. Personally-owned Resources – Any personally-owned resources used for university business are subject to this policy and must comply with all N.C. A&T requirements pertaining to that type of resource and to the type of data involved. The resources must also comply with any additional security requirements specific to the particular university functions for which they are used.

3. Security and Proprietary Information

a. Permitted access to university data – Users shall access university data only to conduct university business and only as permitted by applicable laws, policies, standards and procedures as set forth in the Information Security Policy. Users must not attempt to access data on information resources they are not expressly authorized to access. Users shall not disclose confidential, sensitive or controlled data except as permitted or required by law and only as part of their official university duties.

b. Maintenance of Records – Users shall maintain all records containing university data in accordance with The University of North Carolina General Records Retention and Disposition Schedule and associated guidelines.

b. Security – All physical resources connecting to the university's network must use security software prescribed by the ITS Information Security Services Department to properly secure university information resources and the university's network. Physical resources determined by the university to lack required security software or to otherwise pose a threat to information resources may be immediately disconnected by the university from the university network without notice.

4. Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is a user authorized to engage in any activity that is illegal under international, federal, state or local law while utilizing resources owned, leased or operated by N.C. A&T.

The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

a. Prohibited Use – Users must not send messages or material that are fraudulent, harassing, threatening, or otherwise in violation of law or university policy.

b. Copyrights and Licenses – Users must not violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by N.C. A&T. The illegal distribution of copyrighted material and unlawful file-sharing using the university's information resources are violations of this policy.

c. Political Use – University information resources must not be used for political activities where prohibited by federal, state or other laws, or in violation of university policies.

d. Commercial Use – University information resources should not be used to promote or conduct business for personal use or for other unauthorized commercial purposes, including advertisements, solicitations, promotions or other commercial messages.

e. Service Disruption – Users are prohibited from intentionally disrupting any business, academic or research activities of the university conducted via university information resources. Disrupting activities include, but are not limited to, interfering with normal operations, providing services which interfere with the legitimate function of other resources connected to the university’s network, denial of service attacks, any form of data intrusion or attack, network probing, scanning or sniffing, forged routing information for malicious purposes, and unauthorized access to information resources connected to the university’s network or other networks.

f. Unauthorized Access – Users must not reveal account passwords to others or allow use of their account by others. Users must not attempt to access another user's computer files without said user’s permission or supply false information or identification in order to access another user's account. Users are prohibited from deliberate, unauthorized attempts to access, use or manipulate university computers, secure areas, networks, physical resources, programs or data.

g. Security Measures – Users must not attempt to circumvent, disable or avoid security measures. Users may not use features that exist in technology systems, such as local computer accounts, to bypass or evade security policies or measures. Users are prohibited from using their access

privileges to circumvent or disable security measures in university information resources, to gain access to data or systems beyond the access that has been formally approved by the appropriate parties, to disable features that log or record activities, to remove or destroy such logs or recordings, or make unauthorized copies of university data.

h. Viruses and Malware – Users are forbidden to intentionally use, create or distribute viruses, worms, keyloggers, root kits or other forms of malicious software.

i. Monitoring – Users are forbidden from attempting to intercept or monitor communications on the university network. Users are not to use network monitoring software, sniffers, packet capture systems or other tools to capture, store or analyze network traffic.

j. Theft – Users are prohibited from deliberate attempts to avoid charges for the use of information resources; attempting unauthorized access to computers within or outside the university using the university's information resources or communications facilities; physically or electronically removing any information resource from designated work areas without written authorization; copying, or attempting to copy, data or software without proper authorization; or stealing information resources from the university in any other way.

k. Unapproved Network Devices – Users are prohibited from installing physical or virtual network devices in any location where the university manages the network infrastructure without the express approval of Information Technology Services. Such approval must be received prior to installation.

B. Roles and Responsibilities

Users are responsible for the proper use and protection of information resources as described above.

1. Vice Chancellor of Information Technology Services and Chief Information Officer (CIO)

a. Administration – The CIO is responsible for administering this policy and providing authorization and direction to technical and administrative staff members in accordance with this policy.

2. Authorized Technical and Administrative Staff Members

a. Operations – Authorized technical and administrative staff members take directed action in accordance with this policy to preserve and protect information resources. The normal operation and maintenance of university information resources require authorized staff members to

monitor physical resources and network traffic in accordance with the university's Information Security Policy.

3. Employees, Students, Affiliates and other parties with access to university information resources

a. Authorization – Authorization to use information resources requires that users agree to adhere to this and other applicable policies. N.C. A&T reserves the right to limit, restrict, or extend privileges and access to its resources.

b. Security – Users must physically secure and safeguard information resources within their possession and control. Users must be familiar with and consult information resource policies, standards and procedures as applicable to the user's particular use of information resources. Users must promptly report the theft, loss or unauthorized disclosure of confidential or sensitive information as outlined in the Incident Response Standard.

c. Compliance – Users must use information resources in compliance with the guidance provided by this policy, as well as all applicable laws and university policies, standards, regulations and procedures.

d. Abuse – Users must promptly report any suspected violation of this policy to the ITS Information Security Services department.

C. Warranties and Assurances

N.C. A&T makes no warranties of any kind, whether expressed or implied, with respect to the information resources it provides. The university will not be responsible for damages resulting from the use of information resources, including but not limited to loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a university employee, or by any user's error or omission. N.C. A&T specifically denies any responsibility for the accuracy or quality of information obtained through information resources, except material that is presented as an official university record.

D. Compliance and Sanctions

The university reserves the right to test and monitor security, and to copy and examine any files or information resident on any N.C. A&T information resource to ensure compliance with this policy.

Any violation of this policy will be considered a serious offense and may lead to sanctions as described in the university's Information Security Policy. Sanctions include but are not limited to loss of access to and use of information resources.

E. Cybersecurity Research

Faculty, staff or students engaged in university-sponsored cybersecurity research may obtain an exemption from relevant portions of this policy. Such exemptions will be reviewed and approved by Information Technology Services prior to use of any technology, will be limited to laboratory environments, and will in no way compromise the rules established by this policy or the security, integrity or safety of the university network or any university information resource.

F. Entrepreneurial Activities

The Use of University Resources for Entrepreneurial Activities policy defines the requirements and limitations for using university resources, including information resources, for entrepreneurial activities. Faculty, staff or students engaged in entrepreneurial activities as defined in that policy are exempt from section IV. A. 4. d. of this policy. Violation of the Use of University Resources for Entrepreneurial Activities policy may also constitute violation of this policy. All other sections of this policy remain in force.

G. Conflict with Other Policies

In the event that this policy conflicts with federal or state legislation or with any policy in the UNC Policy Manual, then federal or state law or the UNC policy prevails. If this policy conflicts with another N.C. A&T policy, then the most restrictive rule shall prevail.

V. References

A. University General Records Retention and Disposition Schedule. https://www.ncat.edu/divisions/business-and-finance/policies-misc/rec-ret-pol.pdf

B. N.C. A&T Information Security Policy. https://www.ncat.edu/divisions/its/policy/

Approved by the Board of Trustees

_____

Date policy is effective: Upon approval

First approved: November 16, 2018