REVISED POLICY

NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

SEC. VII – EQUIPMENT USE 3.0

INFORMATION SECURITY

UNIVERSITY POLICY

I. Purpose

This policy sets forth the security requirements for information resources of North Carolina Agricultural and Technical State University (N.C. A&T). This policy explains the administration of the university's Information Security Program, the development and maintenance of security plans, policies and standards, and specific security requirements necessary to comply with federal or state regulations, University of North Carolina System (UNC) policy or contractual obligations.

II. Scope

This policy applies to all information owned or processed by the university, 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 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 Security Program

The Information Security Program is a set of coordinated services and activities designed to protect information resources and manage the risks associated with those resources. It includes policies, standards, assessments, protocols and trainings to govern the storage, accessibility and security of information resources.

C. 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 include data, software and physical assets.

D. Information Resource Custodians

Information Resource Custodians are university employees authorized to grant access to university data based on delegation from an information resource trustee or steward or who have been assigned operational responsibilities for maintaining applicable controls such as data security, physical security, backup and recovery.

E. Information Resource Stewards

Information resource stewards are unit or department leaders with planning and management responsibility for defined information resource data sets, software or physical assets. Data stewardship responsibilities include data classification, access control, accuracy, integrity, retention and disposal.

F. Information Resource Trustees

Information resource trustees are senior university officers (e.g., Vice Chancellors, Vice Provosts, Deans, etc.) who have oversight, policy, and compliance level responsibility for defined information resource data sets, software and hardware resources.

G. University Data

University data are institutional 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.

IV. Policy and Procedure Statements

A. Information Security Program

The university shall develop, implement, and maintain a comprehensive Information Security Program to safeguard the security, confidentiality, accessibility, integrity and availability of university information resources and to address specific security requirements defined by federal and state regulations, University of North Carolina policies, and relevant contractual obligations. Reference: UNC Policy 1400.2

The Information Security Program shall comply with the prevailing information security standard adopted by the UNC Board of Governors. It will produce, at a minimum, policies on the storage, use and accessibility of information resources, operating standards and procedures to document additional technical security requirements, training requirements, regular risk assessments of existing information resources, strategies for prioritizing and managing identified security risks, and procedures for incident response planning and management. These products will be reviewed and updated regularly. Reference: UNC Policy 1400.2, ISO 27002:2013-5.1.1, 5.1.2

Operating standards and procedures produced by the Information Security Program shall contain additional technical requirements and will be an extension of this policy. Adherence to these standards and procedures are mandatory for all employees, students and affiliates.

The Information Security Program will be guided by the following principles:

1. ISO/IEC 27002 – The program shall be guided and informed by the ISO/IEC 27002 standard, adopted as the common security framework for campuses of the University of North Carolina (UNC) System. Reference: UNC Policy 1400.2

2. Legal, Contractual, and Policy Requirements – In relation to the management and protection of information resources, N.C. A&T shall conduct all business in accord with relevant federal and state regulations, University of North Carolina policies, and contractual requirements. The program shall incorporate these requirements into all plans, policies, standards and procedures.

3. Proactive Risk Management – The development of policies, plans, standards, procedures and other products of the Information Security Program shall be driven by the identification, assessment, communication, and efficient and effective treatment of risks related to information resources.

The Information Security Program will be administered in a manner consistent with the roles and responsibilities outlined in section 4.3 of this policy.

B. Governance, Coordination, and Security Services

The Information Security Program will be governed and supported as follows:

1. Information Security Advisory Committee – To ensure that the Information Security Program is aligned to the university mission, values and operational needs, the Information Security Advisory Committee will oversee the collaborative management of the program and development of plans, associated policies, standards, procedures, major initiatives and campus security solutions.

2. Information Security Incident Response Team – To ensure a consistent and coordinated response to information security incidents, an Information Security Incident Response Team will centrally manage all university information security incidents and provide specialized incident response services.

3. ITS Information Security Services Department – To ensure compliance with relevant university information security policies and standards, the ITS Information Security Services Department shall be responsible for providing information security services that help identify risks, establish protective measures, and validate conformance.

C. Roles and Responsibilities

The protection and security of information resources is a responsibility shared by all employees, students and affiliates. All employees, students and affiliates must observe all security related policies, standards and procedures. Reference: ISO 27002:2013-6.1.1

The roles and responsibilities for University Information Security include:

1. Board of Trustees – The Board of Trustees shall be responsible for:

a. Overseeing information security. Reference: UNC Policy 1400.2

b. Approving the university information security policy. Reference: UNC Policy 1400.2

c. Ensuring that information security is addressed in the annual audit plan and risk assessments conducted by the internal auditor. Reference: UNC Policy 1400.2

d. Addressing emerging information security matters. Reference: UNC Policy 1400.2

2. Chancellor and Chancellor's Cabinet – The Chancellor and Chancellor's Cabinet shall be responsible for:

a. Approving the university information security policy.

b. Providing executive oversight and support of the information security program.

c. Providing guidance concerning university risk tolerance levels.

d. Providing resources to meet approved security objectives.

e. Periodically reviewing the university's information security posture.

3. Vice Chancellor for Information Technology Services and Chief Information Officer (CIO) – The Vice Chancellor shall be responsible for:

a. Monitoring the effectiveness of the information security program.

b. Maintaining alignment of Information Technology services with university risk tolerance levels.

c. Periodically reporting the information security posture to the Chancellor and Chancellor's Cabinet.

d. Preparing an annual report on the information security program and information technology security controls. Reference: UNC Policy 1400.2

e. Forming and charging the Information Security Advisory Committee and Information Security Incident Response Team.

4. Director of Information Security Services – The Director of Information Security Services shall be responsible for:

a. Leading the development, execution, and enforcement of the university information security program.

b. Facilitating information security governance and collaboration.

c. Advising senior leadership on security needs and resource investments.

d. Leading the development of information security policies, standards, procedures and guidelines.

e. Maintaining appropriate contacts with relevant authorities, special interest groups, other specialist security forums and professional associations. Reference: ISO 27002:2013-6.1.4

5. Vice Chancellors, Deans, Department Heads and Supervisors – Vice Chancellors, Deans, Department Heads, and Supervisors shall be responsible for:

a. Ensuring that units and applicable affiliates adhere to information security policies and standards. Reference: ISO 27002:2013-7.2.1

b. Ensuring that staff and applicable affiliates receive any required security training. Reference: ISO 27002:2013-7.2.2

c. Ensuring that conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional

modification or misuse of information resources. Reference: ISO 27002:2013-6.1.2

d. Maintaining appropriate contacts with relevant authorities, special interest groups or other forums to meet unit contractual and compliance obligations. Reference: ISO 27002:2013-6.1.4, 6.1.3

6. Office of Internal Auditing

a. Ensuring that information security is addressed in annual audit planning and risk assessment.

7. University Employees, Affiliates and Students – All university employees, affiliates, and students shall be responsible for:

a. Attending all required information security related training.

b. Maintaining awareness and adherence to information security policies and standards.

c. Promptly reporting potential information security incidents to the ITS Information Security Services Department.

D. Control Requirements

Information security risks can be detected, prevented or mitigated by a variety of security controls. Key security requirements for regulatory, policy, and contractual obligations will be addressed through existing controls, compensating controls, or prioritized implementation of new controls consistent with available resources.

1. Risk Management

a. Identification and Analysis – Information resource trustees will regularly identify and analyze risks for information resources.

b. Mitigation – Information resource trustees will implement appropriate controls to mitigate the identified risks.

c. Communication – Information resource trustees will communicate appreciable risks and treatment options on a regular basis for decision review. Reference: ISO 27002:2013-6.1.1; GLBA-16 CFR §314.4; HIPAA-45 CFR §164.308(a) (1)(ii)(A); PCI-DSS 3.0-12.2

2. Human Resource Security

a. Screening/Background Checks – Prospective employees who receive an offer of employment and affiliates who are sponsored to work with the university will be vetted by processes managed by Human Resources.

Reference: ISO 27002:2013-7.1.1; HIPAA-45 CFR §164.308(a)(3)(ii)(B); PCI-DSS 3.0-12.7

b. Security Awareness Training – All university employees will receive regular security awareness training. Employees with specific job responsibilities or roles will receive additional training as required by the Information Security Program. Reference: ISO 27002:2013-7.2.2, PCI-DSS 3.0-12.6

c. Sanctions – Employee and student disciplinary processes and affiliate agreements will include applicable provisions to sanction violations of information security policies or requirements, which may include loss of information resource access privileges, administrative sanctions, and disciplinary actions. Employees, affiliates and students are cautioned that egregious violations may also result in personal civil and criminal liability. Reference: ISO 27002:2013 - 7.2.3; HIPAA: 45 CFR §164.308(a)(1)(ii)(C)

d. Change in Position or Duties – Supervisors will review and make necessary changes to an employee's access to information resources when the employee leaves a position or duties are changed.

e. Termination of Employment or Affiliate Access – Access to information resources, work areas, and secure areas will be revoked, and resources returned upon full separation from the university. Reference: ISO 27002:2013-7.3, 8.1.4; HIPAA: 45 CFR § 164.308(a)(3)(ii)(C); PCI-DSS 3.0: 8.1.3; 9.3

3. Information Resource Management

a. Data Governance – All university data are considered the property of N.C. A&T and will be treated as an information resource. The data stewardship and classification policy defines responsibilities for secure and effective management of university data.

b. Data Classification – The university will use the data stewardship and classification policy to address associated business needs and risks related to sharing or restricting access to university data. Reference: ISO 27002:2013-8.2.1

c. Acceptable Use and Security Requirements – Appropriate utilization of information resources, from on or off campus, will be clearly defined, including secure practices for handling data classified as confidential or sensitive. Reference: ISO 27002:2013-8.1.3,8.2.3, 6.2.2

d. Inventory of Information Resources – An inventory of all physical information resources will be maintained and indicate their steward or custodian, location, and other information necessary for proper

management of the resources. Reference: ISO 27002:2013-8.1.1,8.1.2; HIPAA-45 CFR-§164.310(d)(2)(iii)

e. Removable Media – Removable media must be managed in accordance with the data stewardship and classification policy and related security standards. Reference: ISO 27002:2013-8.3.1

f. Information Resource Transfer and Destruction – Information resources, excluding public data, must be returned upon separation from the university. University data will be appropriately retained and safeguarded for future use. Physical resources will be reliably rebuilt and re-commissioned prior to transfer to another employee. Physical resources will have software and data rendered unreadable prior to sale or other disposition. Reference: ISO 27002:2013-8.1.4,8.3.2, 8.3.3,11.2.7; HIPAA-45 CFR -§164.310(d)(2) (i), §164.310(d)(2)(ii), PCI-DSS 3.0-9.8

4. Access Control

a. Role-Based Access Control – Information resource stewards will define appropriate roles associated with the fulfillment of legitimate business needs. These roles will have associated access control rules, access rights, and restrictions that limit access to confidential and sensitive data while efficiently accomplishing institutional needs. Assignments to these roles and the associated access will be periodically reviewed. Reference: ISO 27002:2013-9.1.1, 9.2.5, 9.4.1; HIPAA-45 CFR-§164.312(a)(1); PCI-DSS 3.0 -7.1

b. Network Access Control – Local and remote access to university networks and information resources will be limited to authorized individuals with legitimate business needs. Reference: ISO 27002:2013-9.1.2; HIPAA-45 CFR-§164.312(a)(1); PCI-DSS 3.0 9.1.2

c. User Access Management – Formal user provisioning and de-provisioning processes will be implemented to ensure that creation of new accounts is authorized, users are uniquely identified, and that user IDs are disabled when no longer required. Reference: ISO 27002:2013-9.2.1,9.2.2, 9.2.6; HIPAA-45 CFR-§164.312(a)(2)(i), §164.312(a) (2)(d); PCI-DSS 3.0-8.1.2

d. Management of Privileged Access – Privileged access rights will be appropriately evaluated, approved, periodically reviewed, and limited to only those users and applications with legitimate and sufficient business need. Utility programs capable of overriding system and application controls will be restricted and controlled. Reference: ISO 27002:2013-9.2.3, 9.4.4; PCI-DSS 3.0-7.1

e. Password Management – Passwords and other authentication methods used to access information resources will be established and managed in a

formally approved and consistently secure manner. Reference: ISO27002:2013-9.2.4, 9.3.1; HIPAA-45 CFR §164.308(a)(5)(ii)(D)

f. Secure Logon – Common secure logon practices will be defined and implemented to ensure that means of access to information resources effectively minimize the risks of unauthorized access threats. Reference: ISO 27002:2013-9.4.2; HIPAA-45 CFR -§164.312(a)(2) (iii)

5. Cryptographic Security (Encryption)

a. Use of Cryptographic Controls – Risks related to the confidentiality and integrity of confidential and sensitive data and non-repudiation of electronic transactions with information resources will be addressed with cryptographic controls. Reference: ISO 27002:2013-10.1.1; HIPAA-45 CFR -§164.312(a)(2)(e); PCI DSS 3.0-3.4

b. Key Management – University cryptographic keys will be generated, stored, and managed in a secure and approved manner. Reference: ISO 27002:2013-10.1.2; PCI-DSS 3.0-3.5,3.6

6. Physical and Environmental Security

a. Physical Security Perimeters and Controls – Secure areas will have well defined physical boundaries and implement sufficient controls to prevent unauthorized entry and physical access. Reference: ISO 27002:2013-11.1.1, 11.1.2; HIPAA-45 CFR §164.310(a)(1); PCI-DSS 3.0-9.1;9.4

b. Environmental Threats – Secure areas will be protected against natural disasters and damage from environmental accidents. Reference: ISO 27002:2013-11.1. 4

c. Safety and Security – Work conducted in secure areas will adhere to all documented safety and security requirements. Reference: ISO 27002:013-11.1.5

d. Removal of Physical Assets – Removal of equipment will be consistent with university policy and will not be taken off-campus without prior authorization. Security will be applied to off-campus assets, taking into account the different risks of working outside the organization's premises. Reference: ISO 27002:2013-11.2.5 11.2.6, 6.2.2; HIPAA-45 CFR §164.310(d)(1)

e. Unattended Equipment – Unattended user equipment will have appropriate protection controls and measures to prevent unauthorized use. Reference: ISO 27002:2013-11.2.8; PCI-DSS 3.0-8.1.8

7. Operations Security

a. Change Management – Changes to information resources and associated processes that impact university information security will be appropriately identified, evaluated, communicated, and controlled. Reference: ISO 27002:2013-12.1.2; PCI-DSS 3.0-6.4

b. Capacity Management – The utilization of critical information resources will be monitored, assessed, and optimized to maximize availability in conjunction with appropriate controls. Reference: ISO 27002:2013-12.1.3

c. Malware Protection – Detection, prevention, and recovery measures will be established to protect information resources against malicious software applications. Reference: ISO 27002:2013-12.2; HIPAA-164.308(a)(5)(ii)(B); PCI-DSS 3.0-5.1

d. Information Backups – Backup copies of university data will be regularly created, retained, stored securely, validated, and periodically tested for recoverability. Reference: ISO 27002:2013-12.3; GLBA-16 CFR 314.4(2); HIPAA-45 CFR §164.310(d)(2)(4);PCI-DSS-9.5.1

e. Logging and Monitoring – Records of important events related to information resources will be reliably retained, reviewed, and protected from tampering and unauthorized access. Reference: ISO 27002:2013-12.4.1, 12.4.2, 12.4.3; HIPAA-45 CFR -§164.312(b); PCI-DSS 3.0-10

f. Clock Synchronization – Clocks of university information systems will be synchronized against a single authoritative reference time source. Reference: ISO 27002:2013-12.4.4; PCI-DSS 3.0

g. Vulnerability Management – Security vulnerabilities related to information resources will be promptly identified, assessed, and remediated according to the associated risks they present to the university. Reference: ISO 27002:2013-12.6

8. Communications Security

a. Network Service Authority – The management and provisioning of university network connections, services, and devices will be limited to staff authorized by Information Technology Services only. Reference: ISO 27002:2013-13.1.1,13.1.2

b. Information Transfer – Transfer methods and controls will be defined and adhered to in order to protect confidential and sensitive information traversing all forms of communication channels to both internal and external senders and recipients. Reference: ISO 27002:2013-13.2.1, 13.2.2; GLBA -16 CFR 314.4(2)

c. Electronic Messaging – Protection measures will be established to safeguard university electronic messaging solutions from unauthorized

access, modification or denial of service. Retention of electronic messaging communication will be maintained in an approved manner. Reference: ISO 27002:2013-13.2.3

d. Confidentiality Agreements – Confidentiality agreements will be used to establish legally enforceable terms of utilization and access for confidential information for both employees and affiliates. Reference: ISO 27002:2013-13.2.4

9. Information Resource Acquisition, Development and Maintenance

a. Security Requirements Analysis – The development and acquisition of information resources will include the regular evaluation of security requirements in the earliest possible stages of related projects. Reference: ISO 27002:2013-14.1.1, 6.1.5.

b. Secure Development – Secure programming techniques and modeling methods will be employed to ensure that coding practices adhere to best practices. Reference: ISO 27002:2013-14.2.1

c. Information Resource Change Control – Change control procedures will be documented and enforced to ensure the confidentiality, integrity, and availability of information resources throughout maintenance efforts. Reference: ISO 27002:2013-14.2.2

10. Supplier Relationship

a. Supplier Security Agreements – Security requirements will be documented and agreed upon with each supplier/external entity that may access, process, store, or communicate university data. Reference: ISO 27002:2013 - 15.1.1, 15.1.2, 13.2.2; GLBA -16 CFR 314(d1); 16 CFR 314(d2)

b. Monitoring and Review of Supplier Services – Periodic review of supplier services will be conducted to ensure that related security agreements are being adhered to and enforced. Hosting providers or other external entities that access, process, store or communicate university data must provide evidence of compliance with this policy or other approved standards. Reference: ISO 27002:2013-15.2.1

11. Information Security Incident Management

a. Reporting of Information Security Events – Information security weaknesses and/or events will be reported through an approved channel and reviewed promptly by authorized employees. Reference: ISO 27002:2013-16.1.2, 16.1.3

b. Management of Information Security Incidents – Response actions

related to security incidents will adhere to a documented set of procedures, including appropriate communication and coordination of efforts. Methods to preserve electronic evidence will follow adequate standards of discovery and preservation to prevent spoliation. Knowledge gained during the analysis of security incidents will be captured, reviewed, and appropriately shared to identify security corrections or control measures that may help address similar events. Reference: ISO 27002:2013-16.1.4, 16.1.5; GLBA -16 CFR 314.4(3) ISO 27002:2013-16.1.6 ISO 27002:2013-16.1.7

12. Business Continuity Management

a. Information Security Continuity – Continuity plans will be developed, reviewed and tested for information resources that are critical for ongoing operations, as identified by information resource trustees and stewards. Periodic verification of these plans will be performed. Reference: ISO 27002:2013-17.1.1,17.1.2,17.1.3

b. Resilient Information Resources – Information software and hardware resources will be implemented with sufficient resiliency to meet identified and documented availability needs. Assessment of these needs will be included in the implementation process. Reference: ISO 27002:2013-17.2

13. Compliance Management

a. Information Security Compliance – The Director of Information Security Services, in consultation with the CIO, shall have primary responsibility for enforcement of the information security policy. The CIO, Director of Information Security Services and the appropriate information resource trustee(s) will address policy violations in accordance with section 4.2.3, utilizing relevant management processes including but not limited to the Faculty Handbook, Student Handbook, Human Resources and the procedures of the Office of State Human Resources.

b. Identification of Compliance Requirements – Regular periodic review will be conducted to ensure that relevant legal, regulatory, policy, and contractual requirements are identified for the university and relevant information resources. Reference: ISO 27002:2013-18.1.1

c. Intellectual Property Rights – Procedures will be implemented to ensure compliance with applicable legal, regulatory, and contractual requirements related to intellectual property rights and use of proprietary information resources. Reference: ISO 27002:2013-18.1.2

d. Protection of Records – University data will be protected from loss, destruction, falsification, and unauthorized release in accordance with legal, regulatory, and contractual business requirements. Reference: ISO

27002:2013-18.1.3

e. Privacy and Protection of Personally Identifiable Information (PII) – The privacy and protection of personally identifiable information will be ensured as required in relevant legal, regulatory and policy frameworks. Reference: ISO 27002:2013-18.1.4

14. Information Security Review

a. Independent Review of Information Security – A qualified independent third party will periodically perform assessment of the university's identification and management of information security objectives. Reference: ISO 27002:2013-18.2.1

b. Compliance with Security Policies and Standards – Periodic assessments will be conducted to review the adherence of university units and employees to applicable information security policies and standards. Reference: ISO 27002:2013-18.2.2

c. Technical Compliance Evaluations – Periodic technical evaluations, including both automated and manual security assessments such as vulnerability and confidential information scanning, will be performed to ensure that technical controls and security measures adhere to applicable information security policies and standards. Vulnerable systems shall be promptly remediated or managed by approved compensating controls. Reference: ISO 27002:2013-18.2.3

Approved by the Board of Trustees

Date policy is effective: April 30, 2018

First approved: April 25, 2014
Revised: , 2018