NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

INFORMATION RESOURCE AUTHENTICATION REQUIREMENTS

UNIVERSITY STANDARD

I. Distribution and Disclosure

This document is a summary of the Authentication Requirements Standard for North Carolina Agricultural and Technical State University (N.C. A&T). This summary is suitable for public disclosure.

The full Authentication Requirements Standard includes information related to the management and security of Information Resources owned or operated by N.C. A&T. The full standard is classified as confidential and is not subject to public records disclosure under North Carolina General Statutes § 132-6.1(c) and/or 132-1.7(b).

Access to the full standard is restricted to employees, contractors and affiliates of N.C. A&T and other individuals as required by federal or State of North Carolina regulation, or contractual obligation, as approved by Information Technology Services. Access to the full standard requires acceptance of a written confidentiality agreement. However, portions of the requirements in the full standard may be made known to Users in order that they may establish Authentication Credentials.

II. Purpose

This Authentication Requirements Standard defines the requirements for Authentication to access Information Resources at North Carolina Agricultural and Technical State University (N.C. A&T). This standard establishes the minimum Authentication Requirements and guidelines for Stewards and Custodians to manage these requirements.

This standard is an extension of the university's Information Security Policy (ISP) and provides additional technical specifications. All requirements and sanctions of these documents apply to this standard.

III. Scope

This standard includes requirements for Authentication at N.C. A&T and applies to all electronic Information Resources that support Authentication. This standard applies to all Information Resources owned or operated by N.C. A&T regardless of location, purpose, college, or division that is responsible for said resource. This includes resources that are housed in facilities owned or operated by third parties. In this event, only those resources owned or operated by N.C. A&T are within the scope of this standard. However, other standards specify the requirements for facilities managed by third parties.

The standard does not apply to environments in which students install, configure, or manage Information Resources as part of instructional assignments. However, if the work includes use of Confidential, Sensitive, or Controlled Data, this standard shall apply. Security requirements for resources that fall under this exclusion are defined in other documents.

Information Technology Services may approve exceptions to any portion of this standard as required to meet operational or technical requirements. All remaining portions shall apply. Exceptions shall not be used to reduce the controls applied to an Information Resource based upon its classification.

IV. Definitions

Authentication – The process of verifying the identity of a User or Information Resource.

Authentication Credentials – Items such as passwords, verification codes, and digital certificates that are used in the Authentication process.

Digital Certificates – A credential that may be used to provide Authentication to access an Information Resource. Certificates are also used for other purposes such as encrypting data sent across a network to protect said data from exposure to third parties. Certificates are typically used in pairs. In this case, one of the certificates is designated as public and can be shared with others while the other must remain private to the User or Information Resource to which it was assigned.

Information Resource – As defined in the ISP, an Information Resource is information owned or processed by the university, or related to the business of the university, regardless of form or location, and the hardware, software, and procedural resources used to electronically store, process or transmit that information. Information Resources expressly include data, metadata, software, processes, procedures and physical assets. Updates to the definition in the ISP shall have precedence over the definition in this standard.

Information Resource Custodians (Custodians) – As defined in the ISP, University employees who have been assigned operational responsibilities for managing compliance with this standard. Updates to the definition in the ISP shall have precedence over the definition in this standard.

Information Resource Stewards (Stewards) – As defined in the ISP, unit or department leaders with planning and management responsibility for compliance with this standard. Updates to the definition in the ISP shall have precedence over the definition in this standard.

Information Resource Users (Users) – Employees, students, and affiliates (as that term is defined in the ISP) authorized to access Information Resources within the scope of the User's employment, affiliation with the university, or enrollment as a student.

Password – A confidential credential typically used to provide a first level of Authentication to access an Information Resource.

Verification Code – A confidential credential with a short lifespan typically presented to a User by a secure channel such as a text message or mobile phone application. Often used to provide a second level of authentication to access an Information Resource.

V. Responsibilities

A. Stewards – Stewards shall observe the requirements of the Access Control Standard IV. B. and shall work with Custodians to ensure that any new Information Resource complies with the requirements of this standard.

B. Custodians – Custodians shall observe the requirements of the Access Control Standard IV. C., shall configure Information Resources according to the requirements of this standard, and shall work with Stewards to ensure that Information Resources comply with this standard.

C. Users – Users shall observe the requirements of the Access Control Standard IV. F. and the requirements below. Users shall promptly notify Information Technology Services and change applicable Password(s) if there is any suspicion of Password compromise.

VI. Requirements

The Access Control Standard outlines requirements for Stewards, Custodians, and Users regarding Authentication. The full Authentication Requirements Standard provides additional requirements regarding the configuration of Information Resources to support Authentication.

The full standard is available to Custodians who configure Authentication. Custodians shall comply with the requirements of the full standard.

VII. Authority, Exemptions, and Advisement

A. Authority and Enforceability – This standard is established under the authority of the university's Information Security Policy and the Vice Chancellor of Information Technology (Information Security Policy IV.C.5).

B. Exemptions – Exemptions to this standard must undergo a formal risk assessment as described in the ITS Risk Management Standard and must be approved in writing by Information Technology Services.

C. Review and Oversight – Collaborative advisement concerning these standards is provided by N.C. A&T technology professionals. The Information Security Advisory Committee (ISAC) is responsible for review, revision, and endorsement of information security standards.

VIII. References

A. ISO 27002:2013 Code of Practice for Information Security Controls

B. UNC Policy 1400.1 Information Technology Governance

C. UNC Policy 1400.3 UNC Policy 1400.1 Information Technology Governance

D. N.C. A&T Information Security Policy

E. N.C. A&T Access Control Standard

Approved by the Chancellor

Date standard is effective: Upon approval
First approved: March 30, 2020