New Standard: This standard defines the requirements to secure and manage servers.

NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

SERVER SECURITY

UNIVERSITY STANDARD

I. Distribution and Disclosure

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

The full Server Security 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.

II. Purpose

The Server Security Standard defines the requirements, practices, and procedures to manage and secure all Servers owned or operated by N.C. A&T, regardless of location, operating system, operating system distribution, or version. The standard is an extension of the university's Information Security Policy (ISP) and Acceptable Use Policy (AUP) and provides additional technical specifications. All requirements and sanctions of these policies apply to this standard.

III. Scope

The Server Security Standard applies to all Servers that are owned or managed by N.C. A&T without regard to the location, or operating system distribution or version. This includes cases in which the operating system or distribution is not classified as a Server operating system, but the computer provides Services as defined within the standard.

In addition to management and security items, the Server Security Standard includes guidelines to ensure Server resiliency and support business continuity efforts.

The Server Security Standard does not apply to Servers that are owned and managed by other organizations that use said Servers to provide Services to N.C. A&T, such as applications hosted on Servers managed by a software vendor. Nevertheless, departments that subscribe to such Services shall obtain evidence of appropriate management and security controls within the hosted environment as required by the N.C. A&T Cloud Security Standard.

Information Technology Services may approve exceptions to any portion of the Server Security Standard that conflicts with the institutional purpose of a Server, such as the learning outcomes of an academic exercise. All remaining portions shall apply. Such exceptions notwithstanding, the Server Administrator shall work with the functional unit and Information Technology Services to implement alternative security measures to protect the Server, the University's network and other University Information Resources. Information Technology Services shall approve the server configuration, including all such measures, prior to server implementation.

IV. Definitions

Administrator – Any person who has been granted permission to use an account with System Privileges, such as the Linux root or Windows Administrator account. The term may also refer to the actual Windows Administrator account.

Server – A computer (container, physical or virtual) running an operating system and applications that provide a service.

Service – A set of computer programs that together provide some functionality or information and are accessible across a network.

System Administrator – See Administrator.

System Privileges – Privileges associated with the management or operation of a Server.

V. Responsibilities

System Administrators – System Administrators are Information Resource Custodians as defined in the ISP. Server Administrators shall fulfill all responsibilities described in the N.C. A&T Access Control Standard as they apply to Servers and Services. System Administrators shall ensure that procedures and tasks 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.

All employees or affiliates who are System Administrators, who have System Privileges, or who manage a server shall observe the requirements of the Server Security Standard.

VI. Standards

This section is only available in the full Server Security Standard.

VII. Configuration Details

This section is only available in the full Server Security Standard.

VIII. Authority

A. Authority and Enforceability – This standard is established under the authority of the university's Information Security Policy and the Vice Chancellor for Information Technology Services.

B. Exemptions – Exemptions to this standard must undergo a formal risk evaluation 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.

IX. References

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

B. UNC Policy 1400.1 Information Technology Governance

C. UNC Policy 1400.2 Information Security

D. UNC Policy 1400.3 User Identity and Access Control

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

F. N.C. A&T Acceptable Use Policy

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

Approved by the Chancellor

Date policy is effective: Upon approval
First approved: August X, 2019