	NORTH CAROLINA A&T STATE UNIVERSITY **CHAPTER 700 – INFORMATION TECHNOLOGY** **UNIVERSITY STANDARD US707,** **VULNERABILITY MANAGEMENT**

SECTION 707.1 STANDARD STATEMENT

Vulnerabilities in Information Resources are a risk to the confidentiality, integrity, and availability of data and to the resources themselves. North Carolina A&T State University's (N.C. A&T or University) Policy 701, Information Security (ISP) requires Information Resource Stewards and Custodians to manage vulnerabilities according to the risks they pose to the University. Information Resource Stewards and Custodians shall use a variety of measures to identify risks and shall ensure prompt assessment and remediation.

SECTION 707.2 PURPOSE

This document defines the standards and practices to identify, assess, and remediate vulnerabilities found in Information Resources.

SECTION 707.3 SCOPE

This standard applies to all Information Resources owned or managed by N.C. A&T without regard to the location, purpose, or type of software or equipment.

SECTION 707.4 DEFINITIONS

"CVSS" means the current version of the Common Vulnerability Scoring System as promulgated by the Forum of Incident Response and Security Teams (FIRST).

"Emergency Change" means a change that must be implemented immediately due to security or availability concerns.

"Information Resource" as defined in ISP means 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. Updates and revisions to the ISP definition shall be considered as adopted in this standard.

"Information Resource Custodian" (Custodian) as defined in the ISP, means any university employee 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, and backup and recovery. Updates and revisions to the ISP definition shall be considered as adopted in this standard.

"Information Resource Steward" (Steward) as defined in the ISP, means 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. Updates and revisions to the ISP definition shall be considered as adopted in this standard.

"Information Resource Trustee" (Trustee) as defined in the ISP, means 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. Updates and revisions to the ISP definition shall be considered as adopted in this standard.

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

"Non-Production Environment" means an environment in which Information Resources are created, modified, or tested to meet the needs of the university. Non-production Environments may be used to test new technologies, new versions or modifications of software, new configurations, or new applications before these resources are deployed in Production Environments. Nonproduction Environments do not support actual university operations.

"Patch" means software supplied by a vendor or developed by Administrators to remediate a particular defect or vulnerability.

"Production Environment" as defined in University Standard US703, Information Technology Change Management Standard, means an environment in which Information Resources are used for university operations. Production Environments are used to support academic, administrative, or research functions and are distinct from Non-production Environments. Updates and revisions to the ISP definition shall be considered as adopted in this standard.

"Vulnerability" means a weakness in a system, either by software defect or configuration, which can be exploited to perform unauthorized actions. Vulnerabilities may or may not result from and may or may not be corrected by patches.

SECTION 707.5 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 707.6 RESPONSIBILITIES

Information Resource Stewards

Stewards are responsible for monitoring a variety of channels to identify Vulnerabilities in Information Resources and ensuring that vulnerabilities are promptly addressed in accordance with this standard.

Information Resource Custodians

Custodians are responsible for monitoring a variety of channels to identify Vulnerabilities in Information Resources, developing remediation plans, and applying Patches, configuration changes, or other steps to promptly address Vulnerabilities in accordance with this standard. Custodians are also responsible for supporting ITS during local system scans, updating configuration documents, and working with ITS to implement compensating controls.

Information Technology Services

Information Technology Services (ITS) is responsible for conducting periodic Vulnerability scans, communicating Vulnerability information to Stewards and Custodians, reviewing and approving remediation plans and compensating controls, and working with the Stewards and Custodians to develop remediation plans as needed.

SECTION 707.7 REQUIREMENTS

Section 707.7.1 Identification

Stewards and Custodians shall use a variety of means to identify Vulnerabilities in Information Resources. These include monitoring communications from vendors and the educational or business community, Vulnerability scans produced by ITS, reports from organizations such as the Cybersecurity and Infrastructure Agency, or other technology resources such as antivirus or antimalware software that may be installed on a resource.

ITS shall conduct periodic network scans of University Information Resources to detect Vulnerabilities. ITS may supplement network scans with local system scans to identify additional vulnerabilities. Stewards and Custodians shall assist ITS with local system scans as needed. ITS shall promptly notify Stewards and Custodians of Vulnerabilities found in resources under their purview as soon as possible but within two (2) business days or discovery.

Stewards and Custodians shall notify ITS of all Vulnerabilities discovered as soon as possible, but within 2 business days of discovery.

ITS shall maintain records of Vulnerability scans for no less than two (2) years.

Section 707.7.2 Assessment

Custodians shall assess each identified Vulnerability and prepare a remediation plan. Assessment shall include changes that are necessary in the configuration of, or services provided by, a resource. The plan shall outline the steps and timeline to address the Vulnerability. Custodians shall submit remediation plans to ITS for review and approval within the timeframes below.

Custodians shall consider the need for an Emergency Change as part of their assessment. In the event that an Emergency Change is authorized, Custodians may forego development of the remediation plan until the change has been implemented. Custodians shall complete forgone plans within five (5) business days once the change is implemented to include in their records.

Remediation plans shall include completion of change management procedures as required by the University's Information Technology Change Management Standard. This includes authorization by the appropriate Steward. Custodians shall update the resource's configuration documents to ensure that changes to remediation vulnerabilities are not subsequently removed.

Remediation plans shall directly address removing Vulnerabilities whenever feasible. In situations where patches or configuration changes are planned but not yet available, or where patching, configuration changes, or other measures such as network isolation are not feasible due to service requirements, the plans should address compensating controls to eliminate or reduce the risk posed by the Vulnerability. In extreme situations, the infeasibility of directly addressing the Vulnerability or implementing compensating controls may require decommissioning of the resource.

In some situations, a patch, configuration change, or other measure becomes available long after the initial identification of the Vulnerability and implementation of the remediation plan. In these cases, the Custodian shall reassess the situation and develop a new remediation plan to use the new capabilities if they offer superior protection. These plans shall be submitted within the timeframes below.

Remediation plans for Vulnerabilities with a CVSS rating of critical or high shall be submitted to ITS within five (5) business days of their identification of the Vulnerability or notice from ITS. Plans for Vulnerabilities with lower CVSS ratings shall be submitted to ITS within fourteen (14) business days. Vulnerabilities that are not given a CVSS rating but are classified as critical, high, urgent, or are considered to pose a significant or immediate risk by the vendor or community members shall be considered as having a critical CVSS score. Other unrated Vulnerabilities shall be considered as having a medium CVSS rating.

Custodians shall maintain records of the assessment, including the remediation plan for no less than two (2) years after the completion of the assessment and remediation plan.

Section 707.7.3 Mitigation

Custodians shall implement remediation plans within fourteen (14) business days of identification or notice from ITS for resources with a critical or high rating. Custodians shall implement remediation plans within thirty business days for Vulnerabilities with a lower score.

Custodians shall review and test the steps taken to address Vulnerabilities to ensure that the Vulnerabilities are successfully remediated. If the Vulnerability was discovered by an ITS scan, ITS shall rescan to verify the successful remediation. Vulnerabilities that are not successfully addressed shall be remediated within five (5) additional business days.

Stewards and Custodians shall consult with ITS if Vulnerabilities cannot be addressed in the respective timeframes outlined in this document. ITS shall work with the Steward and Custodian to develop a remediation plan with an extended timeline. However, delays in addressing Vulnerabilities shall be as limited as possible and shall be developed on a case-by-case basis.

Custodians shall maintain mitigation plans and mitigation records for at least two (2) years from completion of the mitigation.

Section 707.7.3 Emergency Changes

University Standard US703, Information Technology Change Management states that Emergency Changes shall only be applied to address an immediate threat to an Information Resource in a Production Environment. Authorization of the Emergency Change must be provided by the appropriate Steward(s), or the appropriate Trustee(s), the Vice Chancellor for Information Technology (CIO), or the CIO's designee in the absence of the Steward(s).

SECTION 707.8 EXCEPTIONS

This standard does not apply to Information Resources owned or managed by other organizations that use those resources to provide services to N.C. A&T. Departments that subscribe to Information Resources owned or managed by other organizations services shall obtain evidence of appropriate vulnerability management controls from the service provider.

This document does not apply to Information Resources in a laboratory environment used for instruction or research that is segmented or physically separated from the rest of the University network. Segmentation of those resources shall include limitations on access from those resources to other parts of the University network and the Internet. These limitations shall be developed in cooperation with, and approved by ITS before the resources are connected to any N.C. A&T network. Physically separated equipment resources 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 Information Resources. All remaining portions shall apply. When exceptions are approved, the Stewards and Custodians shall work with the functional unit and ITS to implement alternative security measures to protect the resource, the University's network, and other University information resources. ITS shall approve the configuration, including all alternative measures, prior to connecting any resource to a University network.

Exceptions from 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 Standard US703, Information Technology Change Management