NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

INFORMATION RESOURCE RISK CLASSIFICATION

UNIVERSITY STANDARD

I. Purpose

This standard defines the requirements to classify Information Resources according to risk at North Carolina Agricultural and Technical State University (N.C. A&T). Risks associated with the use of Information Resources include data exposure, data loss, data corruption, or exploitation as a platform from further attacks resulting from a system compromise. Additional risks include the potential impact on the operations of the university or of a unit resulting from the damage or destruction of a resource. Proper classification ensures that the appropriate controls are used to secure and protect Information Resources. Classification also ensures that Information Resources critical to operations are identified so that recovery or business continuity measures can be implemented.

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

II. Scope

This document defines requirements for classification for 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.

This 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 policies or standards.

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.

III. Definitions

Confidential Data – As defined in the ISP, data that are protected by federal, state, or local statutes and regulations, industry regulations, provisions in government research grants, or other contractual arrangements, which impose legal and technical restrictions on the appropriate use of institutional information. This includes data covered by data breach notification laws or contractual provisions in government research grants, which impose legal and technical restrictions on the appropriate use of institutional information. Confidential Data includes personally identifying information, personal health information, confidential research data and other data that has been classified as confidential through the ISP. Updates to this definition in the ISP shall have precedence over the definition in this standard.

Controlled Data – As defined in the ISP, data that is proprietary or produced only for use by members of the university community who have a legitimate purpose to access such data. Access to Controlled Data is protected, requires general security requirements, and is provided only for the fulfillment of normal position requirements. Updates to this definition in the ISP shall have precedence over the definition in this standard.

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 Custodian (Custodian) – As defined in the ISP, 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. Updates to this definition in the ISP shall have precedence over the definition in this standard.

Information Resource Steward (Steward) – As defined in the ISP, 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. Updates to this definition in the ISP shall have precedence over the definition in this standard.

Information Resource Trustee (Trustee) – As defined in the ISP, 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. Updates to this 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.

Public Data – As defined in the ISP, university data that have few restrictions and/or are intended for public use. Updates to this definition in the ISP shall have precedence over the definition in this standard.

Sensitive Data – As defined in the ISP, data that is non-regulated, but considered private and protected by contracts, third-party agreement, or the university for restricted treatment. Sensitive Data includes personal data for applicants, students, parents, donors and alumni, as well as research and other institutional data that the university has agreed to keep private. Updates to this definition in the ISP shall have precedence over the definition in this standard.

IV. Responsibilities

A. Trustees – Trustees shall ensure that all Information Resources under their purview are classified according to this standard, and that all classifications are reviewed and updated as needed. Review shall occur following major changes to Information Resources, but no less than annually. Trustees shall ensure that Stewards and Custodians identify the risks associated with and apply the appropriate controls to Information Resources in cooperation with ITS.

B. Stewards – Stewards shall ensure that all Information Resources under their purview are classified according to this standard, and that all classifications are reviewed and updated as needed. Review shall occur following major changes to Information Resources, but no less than annually. Stewards shall work with Trustees and ITS to identify risks associated with Information Resources, shall communicate the classifications to ITS, and shall ensure that Custodians apply the appropriate controls to Information Resources in cooperation with ITS. Stewards shall ensure that Users are informed of the classification of Information Resources which they access.

C. Custodians – Custodians shall provide Stewards with any and all information required for accurate classification of Information Resources and shall apply the appropriate controls to Information Resources in cooperation with ITS.

D. Users – Users shall provide Stewards and Custodians with timely notification of issues with or changes to Information Resources. Users shall make themselves aware of the classification of Information Resources which they use.

E. ITS – ITS shall manage and maintain Information Resource Risk Classification processes, support and train Stewards and Custodians in their responsibilities under this standard, and specify the appropriate controls for Information Resources based on their classification. ITS shall also resolve any cross-functional issues arising from resource classification.

V. Requirements

All N.C. A&T Information Resources shall be classified according to the requirements of this standard. Risk classification shall occur during the initial deployment of the resource and shall be reviewed and updated as needed. Review shall occur following major changes to Information Resources, but no less than annually.

Stewards shall work with Trustees and ITS to identify the risks associated with Information Resources and the severity of their compromise or failure, shall determine the classification of those resources, and shall provide this information to ITS.

Risk classification shall be used to determine the appropriate security controls for each Information Resource. ITS shall identify these controls and work with Stewards and Custodians to implement them.

Information Resource Risk Classification is separate from but may be affected by data classification, as outlined below.

A. Information Resources shall be classified as Low Risk, Moderate Risk, or High Risk. A resource's sole classification shall be the highest risk determined by the three factors in the table below.

B. Information Resources Risk Classification factors include data, role, and failure or compromise. These factors are summarized in the table and explained in more detail below.

Risk Classification	Data	Role	Failure or Compromise
Low Risk	Stores, processes, or transmits Public Data only.	Interacts with the general public or other external groups. Business with the university is not covered by specific regulations, laws, or contractual agreements.	Little impact on the operations, compliance, reporting, safety, finances, reputation, or strategic plans of the university. See below for additional guidelines.

Moderate Risk	Stores, processes, or transmits Public or Controlled Data.	Interacts with specific groups of Users who are assigned limited access based on their roles. Interaction excludes exchange of Confidential or Sensitive Data. See below for additional guidelines.	Limited impact on the operations, compliance, reporting, safety, finances, reputation, or strategic plans of the university. See below for additional guidelines.
High Risk	Stores, processes, or transmits Confidential or Sensitive Data.	Interacts with specific groups of Users who are assigned limited access based on their roles and Confidential or Sensitive Data is exchanged. See below for additional guidelines.	Serious impact on the operations, compliance, reporting, safety, finances, reputation, or strategic plans of the university. Failure or compromise would require the university to report to an external party or notify an affected individual. See below for additional guidelines.

C. Information Resources shall be rated based on the data that they store, process, or transmit according the data definitions listed in the ISP.

1. Low Risk – The resource, stores, processes, or transmits Public Data.

2. Moderate Risk – The resource, stores processes, or transmits Controlled Data.
3. High Risk – The resource stores, processes, or transmits Confidential or Sensitive Data.

4. Computer systems store a network configuration, and most are capable of storing passwords for local accounts. Both are classified as Confidential Data. For the purposes of this rating, network configurations and local account passwords should be excluded from consideration, unless the primary purpose of the resource is to manage network configurations or accounts. This exclusion notwithstanding, these elements of a resource shall be protected by the appropriate controls outlined in other standards.

D. Information Resources shall be rated based on the role or purpose of the resource.

1. Low Risk – The role or purpose is intended for interaction with the general public or other external groups whose business with the university is not covered by specific regulations, laws, or contractual agreements. Interaction does not include the exchange of personally identifiable or other information that is not available to the general public. In addition, the role or purpose does not include the health and safety of employees, students, affiliates, or visitors and excludes the protection of other Information Resources.

2. Moderate Risk – The role or purpose is intended for interaction with specific groups of Users who are assigned limited access based on their roles, or with other Information Resources, but the interaction excludes exchange of Confidential or Sensitive Data. In addition, the role or purpose does not include the health and safety of employees, students, affiliates, or visitors and excludes the protection of other Information Resources.

3. High Risk – The role or purpose is intended for interaction with specific groups of Users who are assigned limited access based on their roles, or with other Information Resources, where the interaction includes exchange of Confidential or Sensitive Data. Alternatively, the role or purpose includes protection of the health and safety of employees, students, affiliates, or visitors, or includes protection of the security and integrity of other Information Resources.

E. Information Resources shall be rated based on the risk or impact posed to operations by failure or compromise of the resource. Failure may include an unplanned service outage or the damage or destruction of the resource.

1. Low Risk – The failure or compromise poses little impact on the university. The failure or compromise will not disrupt operations of any department and will not result in any of the adverse effects described below. System compromise by an attacker would not expose any portion of the university's network to the intruder.
2. Moderate Risk – The failure or compromise poses limited impact on the university. Failure or compromise will disrupt the operations of a single department. Failure or compromise would not result in noncompliance with federal or state regulations or contractual requirements, would not jeopardize the safety or security of an online or physical environment, would not require the university to report to an external party or notify an affected individual, would not incur financial penalties or damages, and would not hinder the implementation of the university's strategic plan in any significant way. System compromise by an attacker would expose a limited portion of the university's network containing low or moderate risk resources to the intruder.

3. High Risk – The failure or compromise poses serious impact on the university. The failure or compromise will disrupt the operations of multiple departments, result in noncompliance with federal or state regulations or with contractual requirements, or jeopardize the safety or security of an online or physical environment. Alternatively, the failure or compromise will require the university to report to an external party or notify an affected individual, incur financial penalties or damages, harm the university's reputation, or hinder the implementation of the university's strategic plan. System compromise by an attacker would expose a significant portion of the university's network or additional High Risk resources to the intruder.

F. Enterprise Information Resources that are critical to the operation of the university shall be designated as High Risk. Examples include N.C. A&T's network, email, telephony and other communication systems, and enterprise applications used throughout the university.

G. Risk Classification of Information Resources shall be informed by a formal risk assessment when necessary, as specified in the Information Resource Risk Management Standard.

H. Risk Classification of Information Resources shall be included in Information Resource inventories, as specified in the Information Resource Inventory Standard.

VI. 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. Exceptions – Exceptions to this standard must undergo a formal review and be approved in writing by Information Technology Services.

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

VII. References

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

B. UNC Policy 1400.1 Information Technology Governance

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

Approved by the Chancellor

Date policy is effective: Upon approval

First approved: March 30, 2020