New Standard: This standard defines the access control requirements for university information resources and the responsibilities of information resource trustees, stewards, custodians, supervisors, and users.

NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

ACCESS CONTROL

UNIVERSITY STANDARD

I. Purpose

This standard defines the requirements to facilitate authentication, authorization, access control, and auditing of Information Resources owned or operated by North Carolina Agricultural and Technical State University (N.C. A&T). It defines the responsibilities of Information Resource Trustees, Stewards, and Custodians who oversee or manage Information Resources and the responsibilities of Users who access and use them. It also defines the Logical and Physical Access Control measures required for all Information Resources.

The purpose of this standard is to ensure the confidentiality, integrity, and availability of university resources, and to ensure compliance with federal and state regulations, University of North Carolina (UNC) system policies, and contractual obligations.

This 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.

II. Scope

The standard applies to all Information Resources owned or operated by N.C. A&T regardless of location, including data, software, and physical resources. It also applies to applications, systems, or services that contain the university's data but are not owned, managed, or operated by N.C. A&T. Some requirements of this standard apply to common desktop or mobile applications that do not require authentication to use and may be classified as utility systems, such as word processors or spreadsheet programs. Many more requirements apply to these applications when they are used to create, analyze, process, present, or otherwise manipulate Confidential, Sensitive or Controlled Data, and to files produced by these applications that contain this data in detailed or summary form. Responsibilities specified in this standard apply to Users who are authorized to use Information Resources as well as all employees responsible for authorizing and managing access to Information Resources.

Information Technology Services may approve exceptions to any portion of this standard only when a business need exists, the exception is necessary to fulfill the goals and objectives of the university, and a risk assessment has been completed. All remaining portions of this standard shall apply. Such exceptions notwithstanding, the appropriate Information Resource Steward shall work with Information Technology Services and Users to implement alternative security measures to protect the university's Information Resources. Information Technology Services shall approve all such exceptions and Compensating Controls prior to implementation.

III. Definitions

Access – The ability to use, modify or manipulate an Information Resource or to gain entry to a physical area or location.

Access Control – The use of administrative, physical, or technical security features to manage the methods Users and systems employ to communicate and interact with Information Resources.

Authentication – The processes by which a User's identity is established and presented to an Information Resource.

Authorization – The processes to grant Users specific privileges to use Information Resources. Authorization refers to both the institutional processes of identifying and approving specific access privileges as performed by Information Resource Stewards and the technical processes of establishing these privileges in a User session as performed by an application or system.

Compensating Controls – A control employed in lieu of the normal and recommended control that provides equivalent or comparable protection for an Information Resource.

Confidential Data – As defined in the N.C. A&T Information Security Policy, data that is controlled by federal, state, local, and/or industry regulations, or by contractual agreement. These data are affected by data breach notification laws and contractual provisions in government research grants, which impose legal and technical restrictions on the appropriate use of institutional information. Confidential Data includes personal identifying information, personal health information, confidential research data and other data that has been classified as

confidential through the Information Security policy. Updates to this definition in the Information Security Policy shall have precedence over the definition in this standard.

Controlled Data – As defined in the N.C. A&T Information Security Policy, 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 Information Security Policy shall have precedence over the definition in this standard.

Information Resource Custodians – As defined in the N.C. A&T Information Security Policy, 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 Information Security Policy shall have precedence over the definition in this standard.

Information Resource Stewards – As defined in the N.C. A&T Information Security Policy, 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 Information Security Policy shall have precedence over the definition in this standard.

Information Resource Trustees – As defined in the N.C. A&T Information Security Policy, 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 Information Security Policy shall have precedence over the definition in this standard.

Logical Access Control – The use of application, system, network, or other technology features to limit connections to data, software or physical resources.

Physical Access Control – The use of physical barriers and security features to limit access to buildings, rooms, closets and other areas with data, software or physical resources.

Principle of Least Privilege – The principle of limiting User access to only those resources necessary for completion of assigned duties or functions, and nothing more.

Principle of Separation of Duties – The principle of ensuring that no single party has responsibility for completing or controlling a set of tasks from beginning to completion whenever this responsibility involves the potential for fraud, abuse, or other harm. This includes ensuring that no single party can approve his or her own access to modify or delete data.

Privileged Access – Access that affords a greater degree of control over Information Resources, such as the ability to modify configuration settings, create or modify User accounts, modify User access privileges, modify authentication credentials, and perform other administrative tasks

associated with the resource. Examples include application, system, network, or database administrators and developers who require a higher degree of access in order to accomplish the duties of their positions.

Role-Based Access – A principle whereby a User is granted access to data, applications, systems or networks based on the roles and duties of that individual within the University.

Sensitive Data – As defined in the N.C. A&T Information Security Policy, data that is non-regulated, but considered private and protected by contracts, third-party agreement, or the University for restricted treatment. Unauthorized disclosure, alteration, or destruction of this data type could cause a significant level of risk to the University or its affiliates. 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 Information Security Policy shall have precedence over the definition in this standard.

Service Account – A specialized account designed for use only by a background process or application to interact with a system. Service Accounts are not User accounts and are not intended for interactive or batch use by administrators or other employees.

Shared User ID – An account created for a work entity or group such as a department or organization for the purposes of accessing an Information Resource.

User Account or User ID – An account assigned to a specific person for the purposes of accessing an Information Resource.

User Endpoint – Any virtual or physical desktop, laptop, tablet or similar device running an operating system whose primary purpose and use is to interact with a user.

Users – Employees, affiliates or students who access and use university Information Resources.

IV. Responsibilities

A. Information Resource Trustees – Information Resource Trustees are responsible for oversight, policy, and compliance of Information Resources under their purview. Trustees shall observe the following requirements:

1. Assignment of Information Resource Stewards – Information Resource Trustees shall assign Information Resource Stewards the responsibility to control, authorize, and audit access to resources under their purview.

2. Separation of Duties – Information Resource Trustees shall ensure that the Principle of Separation of Duties is followed when assigning Information Resource Stewards and shall promptly address any situation where this principle is not in force.

3. Fulfill Steward Responsibilities – Information Resource Trustees shall fulfill the duties and responsibilities of an Information Resource Steward as needed.

B. Information Resource Stewards – Information Resource Stewards are responsible for planning and management of Information Resources under their purview. While stewards have broad responsibilities described throughout this standard, their key responsibilities are summarized below.

    1. Information Resource Access – Information Resource Stewards shall control, authorize, and audit access to all Information Resources assigned to them by the appropriate Information Resources Trustee.

    2. Role-Based Access – Information Resource Stewards shall ensure that role-based access is used to provide access to relevant Information Resources in accordance with the work duties of each User.

    3. Least Privilege – Information Resource Stewards shall observe the Principle of Least Privilege and ensure that Users have access to those Information Resources required for the duties of a User's position and no more.

    4. Accountability – Information Resource Stewards shall ensure that User IDs are assigned, and that Information Resources are configured in such a manner as to provide accountability of individual Users.

    5. Formal Procedures and Records – Information Resource Stewards shall ensure that formal procedures are documented and followed to execute their responsibilities as described in this standard, and that records of these actions are maintained for review in information security assessments, audits or other reviews.

    6. Procurement – Information Resource Stewards shall work with Information Technology Services to ensure that new or updated applications, systems, and services are capable of meeting the requirements of this standard.

C. Information Resource Custodians – Information Resource Custodians are authorized to grant access or have operational responsibilities for maintaining controls in Information Resources. While custodians have broad responsibilities described throughout this standard, their key responsibilities are summarized below.

    1. Information Resource Access – Information Resource Custodians shall create and manage User IDs and access as approved by Information Resource Stewards.

    2. Accountability – Information Resource Custodians shall support Information Resource Stewards in ensuring accountably of individual Users.

    3. Authentication and Authorization – Information Resource Custodians shall ensure that authentication credentials and access privileges are managed and protected as described in this standard, and that User IDs and access are approved by the appropriate Information Resource Steward.

4. Configuration – Information Resource Custodians shall work with Information Technology Services to ensure that new or updated applications, systems, and services are configured to comply with the requirements of this standard.

5. Monitoring – Information Resource Custodians shall monitor Information Resources and ensure that User IDs and access privileges remain consistent with those approved by Information Resource Stewards.

6. Retention of Files and Data – Information Resource Custodians shall ensure that business files and data are retained and transferred to the appropriate member of a department as needed to support the business operations of the University.

7. Access Modification and Account Termination – Information Resource Custodians shall ensure that access is promptly updated or removed when Users change positions or User IDs are disabled when Users separate from the University.

8. Formal Procedures and Records – Information Resource Custodians shall ensure that formal procedures are documented and followed to execute their responsibilities as described in this standard, and that records of these actions are maintained for review in information security assessments, audits or other reviews.

D. Supervisors – All supervisors and affiliate sponsors shall observe the following requirements:

1. Authorization – Supervisors and sponsors shall work with Information Resource Stewards to authorize employee or affiliate access sufficient to allow them to fulfill legitimate duties of their position. Supervisors and sponsors shall work with Stewards to limit access based on the Principle of Least Privilege and approve no more access than that necessary for position responsibilities.

2. Access Review – Supervisors and sponsors shall work with Information Resource Stewards to review and make necessary changes to employee or affiliate access when a person separates from a position or when duties are changed.

3. Employee Separation – Supervisors and sponsors shall communicate employee or affiliate last work dates to Human Resources as soon as said dates are known or anticipated so that User IDs and access privileges can be promptly deactivated.

4. Security Training – Supervisors and sponsors shall ensure that all Users attend general and specialized information security training as required for their position.

5. Separation of Duties – Supervisors and sponsors shall assist Information Technology Trustees in identifying situations where the Principle of Separation of Duties is not in effect and shall assist Trustees in resolving these matters as needed.

E. Shared User ID Managers – Users who manage access to Shared User IDs or who have access to Shared User IDs shall observe the requirements to manage, protect, share and

change authentication credentials of Shared User IDs as explained in the Authentication and Privileged Access Management sections.

F. Users – All Users shall observe the following responsibilities:

1. Secure Access – Employees, students and affiliates authorized to access University information are responsible for properly securing Information Resources from unauthorized access, as well as for securing and protecting passwords, keys, and other forms of Access Control. This includes ensuring that data is encrypted during transmission or transport.

2. Clear Desk – Users who handle Confidential, Sensitive or Controlled (CSC) Data shall adequately conceal this information from unauthorized disclosure to non-authorized parties. Unless information is in active use by authorized personnel, desks must be clear of CSC data. During non-working hours all CSC data shall be stored in a locked location inaccessible to unauthorized parties.

3. Clear Screen – Users shall deploy measures to prevent unauthorized access when they leave their computer station unattended. Computers shall be configured with a time-activated screen and keyboard locking mechanism controlled by a password or similar user authentication mechanism to minimize the chances of unauthorized access to unattended equipment. This shall include laptops, tablets, smartphones, desktops, servers, and similar devices.

   To further safeguard CSC data, Users with access to said information shall proactively lock their computer station before leaving the machine unattended.

4. Computer Security – Users shall log off computers or ensure that said computers are configured to enter sleep mode when not in use. Computers shall require authentication when waking from sleep mode. Users shall shut down computers when not in use.

5. Unauthorized Access – Users shall not attempt to access any Information Resource for which they have not been granted permission and shall promptly report any such access to the Department of Information Security Services. This includes instances in which they determine that they have access to an Information Resource which they believe was not explicitly granted.

6. Authentication – Users shall protect all credentials used to authenticate with an Information Resource, such as passwords, personal identification numbers (PINs) or other codes or credentials. Users shall not share passwords with another entity, shall not use passwords of other Users, and shall promptly report any such activity to the Department of Information Security Services.

V. Requirements

A. Access Privileges – Access to Information Resources belonging to N. C. A&T is a privilege. Employees, affiliates and students shall observe all policies, standards, procedures, and other

requirements. Violation of these items may lead to revocation of access privileges or other sanctions as outlined in relevant policies.

B. Role-Based Access – Access to Information Resources is restricted and shall be approved by the appropriate Information Resource Steward before Users may access said resources. Access shall be based on identities and roles and shall observe the Principles of Least Privilege and Separation of Duties.

1. Information Resource Stewards shall approve access to Information Resources based on identities and roles. Stewards shall follow the Principle of Least Privilege and only grant access to Users whose work duties and responsibilities require such access. Stewards shall grant the minimum access required to perform the work duties and no more. If this is impossible or infeasible, stewards will work with Information Technology Services to implement Compensating Controls.

2. In specific cases, Users may be granted access to Information Resources based on their role without application or additional approval by an Information Resource Steward. Such access must include provisions to ensure that Users only access data that is their own or that they have a business reason to access. Examples of said access include access to learning management or email systems, access to computer laboratory computers, or access to a self-service application. Access to a public web site is another example and is granted to any individual, even those without a relationship to the University.

C. User ID Management – User IDs are assigned to an individual to facilitate Authentication, Authorization, Access Control, and Auditing. Information Resource Stewards and Custodians shall maintain formal, written procedures for the assignment, management and retirement of User IDs within the resources under their purview. Stewards shall use the unique University identity known as OneID assigned by Information Technology Services whenever possible. Procedures for managing user IDs shall ensure that the requirements below are met.

1. Information Resource Stewards will assign a unique User ID to an individual upon approval of access for all resources under their purview.

2. Information Resource Stewards shall ensure that actions of Users can be recorded within the resources under their purview to ensure individual user accountability.

3. Information Resource Stewards shall immediately disable User IDs when Users separate from the University, or when duties change to the extent that access is no longer required. For extended access exceptions to this requirement, see the section on Authorization.

4. Information Resource Stewards shall monitor the assignment and management of User IDs and ensure that any errors, redundant IDs, and other anomalies are promptly corrected.

5. Information Resource Stewards shall not assign individual User IDs for use by a Service Account. Information Resource Custodians and Users shall not use User IDs for Service Accounts.

6. In cases where Service Accounts are not preconfigured within an application or system, Information Resource Stewards shall work with the appropriate Information Resource Custodians to assign a unique User ID.

7. Whenever possible, Information Resource Stewards shall ensure that User IDs assigned to Service Accounts are distinguishable from User IDs assigned to Users.

8. Shared User IDs are permitted in cases where individual User IDs are impossible or infeasible. Information Technology Services and the appropriate Information Resource Steward must approve the exception to create and use a Shared User ID. Requests for Shared User IDs must be accompanied by a valid business justification. Trivial justifications such as a minor reduction in the workload of an Information Resource Custodian are not acceptable.

9. Information Resource Stewards shall assign a Shared User ID to a specific User. Said User shall manage access to and use of the Shared User ID, and is responsible and accountable for all actions taken by the Shared User ID. See the section on Authorization for additional requirements.

D. Authentication – All Information Resources except those designated for public access shall require Users to authenticate in order to confirm their identity and establish Authorization within a user session. Information Resource Stewards, Custodians, and others with access to Authentication credentials shall observe the following requirements:

1. Users are accountable for all actions performed using their User ID and shall protect Authentication credentials from intentional or accidental disclosure. Users shall not share credentials and shall not use credentials of other Users.

2. Information Resource Stewards and Custodians shall ensure that applications and systems use encryption to transmit and store Authentication credentials. Whenever possible, applications and systems shall be configured to store credentials in a manner that prevents decryption.

3. Information Resource Stewards and Custodians shall ensure that unique initial credentials are provided through a secure channel in such a way that they remain confidential. Initial passwords shall be changed upon first logon.

4. Information Resource Stewards and Custodians shall ensure that all vendor-supplied default or blank passwords are immediately identified and reset upon installation of the affected application, device, or system.

5. Information Resource Stewards and Custodians shall ensure that all Authentication credentials for Service Accounts and local accounts within applications or systems are changed whenever a User who has knowledge of or access to the credentials separates from the University or when duties are changed to the extent that access to the credentials is no longer warranted.

6. Information Resource Stewards, Custodians and Users shall ensure that Authentication credentials are not stored in clear text or in any easily reversible form. Credentials shall only be coded into programs or queries in an encrypted form. Exceptions to this requirement are permissible only when no other reasonable option exists.

7. Information Resource Stewards and Custodians shall ensure that all Information Resources use the NCAT Active Directory domain (ncat.edu) for authentication. In cases where this is impossible, infeasible or inadvisable, Stewards and Custodians shall implement controls over User IDs and Authentication credentials consistent with those in the NCAT domain. Other Active Directory domains are prohibited, except in instances where said domain is used for instruction, research, or the testing of new technology.

8. Information Resource Custodians shall ensure that all applications and systems that store or process CSC data use two-factor authentication whenever possible. Custodians shall use two-factor authentication mechanisms provided by Information Technology Services whenever possible. Custodians shall work with Information Technology Services to establish Compensating Controls for resources that store or process CSC data but that are unable to use two-factor authentication.

9. Information Resource Custodians who manage a Shared User ID shall ensure that Users with access to the Shared User ID use software tools such as the Linux sudo command to access the Shared User ID whenever this is technically feasible. In these cases, the custodian shall not distribute the actual Shared User ID password or other authentication tokens.

10. Users who manage a Shared User ID shall fulfill the relevant duties of an Information Resource Steward or Custodian as described in this standard. Said Users shall control access to the credentials of the shared account, distribute these credentials only to other Users authorized by the appropriate Steward, and maintain a written history of all Users who have access to the credentials and of changes in credentials. Said Users shall work with the appropriate Custodian to immediately change credentials if an authorized User separates from the University or moves to a role that no longer requires access to the Shared User ID. Said Users shall also ensure that credentials are changed according to the normal expiration period in use at that time.

E. Authorization – Information Resource Trustees and Information Resource Stewards shall ensure that the Authorization processes to grant access privileges to Users follow the role-based Access Control principles described above. Trustees and Stewards shall observe the following Authorization requirements:

1. Information Resource Trustees shall designate Information Resource Stewards to control and authorize access for all Information Resources under their purview.

2. Information Resource Trustees shall observe the Principle of Separation of Duties in the Authorization process. Trustees shall ensure that no individual has overlapping responsibility for requesting, authorizing and provisioning access to Users. If this is not possible or feasible, Trustees shall work with Information Technology Services to implement Compensating Controls.

3. Information Resource Trustees shall authorize the access of Information Resource Stewards by identifying them and assigning responsibility to manage and control access to specific resources.

4. Information Resource Stewards shall ensure that formal procedures to grant, remove, review, and audit User access are documented and followed.

5. Information Resource Stewards shall compile individual access privileges to Information Resources into collections or classes that reflect typical User roles or profiles whenever possible. Each collection or class shall enable Users to perform the minimum set of defined actions for their role and shall restrict access based on the Principle of Least Privilege.

6. Information Resource Stewards shall review privilege assignments every six months for applications or systems that store CSC data, and at least annually for other resources. Reviews shall include assessment of privileges assigned to each collection or class, and each user assignment to a collection or class. Stewards shall modify access as needed following review to comply with the requirements of this standard.

7. Information Resource Stewards may authorize access to Users after they separate from the University or change duties when said access is beneficial to the University or contributes to conducting university business. Access must be requested and justified by the persons supervising such Users and approved by the appropriate Information Resource Stewards.

8. Information Resource Stewards shall maintain records of all access management activities and ensure that said records are available during information security assessments or audits.

F. User Access Provisioning – Information Resource Stewards shall ensure that formal procedures are documented and followed to control the allocation of access privileges to Information Resources. The procedures must cover all stages in the life cycle of User access, from the initial registration of new Users to the final deactivation of User access that is no longer required. Provisioning processes must include the requirements below.

1. Information Resource Stewards shall ensure that employees and affiliates follow an access application process and that supervisors approve and authorize employee or affiliate access consistent with the User's job responsibilities.

2. Information Resource Stewards shall authorize employee or affiliate access privileges required for the User's role. Stewards shall ensure that the level of access granted is consistent with the requirements of this standard.

3. Information Resource Custodians shall ensure that access privileges are implemented correctly and are not activated before Authorization procedures are completed.

4. Information Resource Custodians shall review access privileges after they have been implemented and immediately correct any errors or mistakes.

5. Information Resource Custodians shall ensure that business files and university data are retained and transferred to the appropriate department following deactivation of or changes in User access.

6. Information Resource Stewards and Custodians shall maintain a record of access provisioning actions for review during information security assessments or audits.

7. Users shall accept all applicable confidentiality and security requirements when applying for access and prior to approval by the supervisor and Information Resource Steward.

8. Supervisors shall promptly notify Human Resources to ensure the immediate removal or modification of access privileges for Users who have separated from the University or moved to new duties that do not require the same access.

9. Human Resources shall promptly notify all Information Resource Stewards and Custodians of Users who have separated from the University or moved to new duties.

G. Privileged Access Management – Privileged Access affords a greater degree of control over Information Resources. The inappropriate use or abuse of Privileged Access is a major contributory factor to system failures and security breaches. Consequently, Privileged Access requires additional management measures. Information Resource Stewards and Information Resource Custodians shall ensure that the requirements below are met.

1. Information Resource Stewards shall tightly control Privileged Access and assign access to Information Resource Custodians or other Users following the Principles of Least Privilege and Separation of Duties.

2. Information Resource Stewards shall ensure that employees and affiliates follow an access application process, that supervisors approve the assignment of Privileged Access consistent with the job responsibilities of their employees, and that Information Technology Services approves Privileged Access applications.

3. Information Resource Stewards and Custodians shall assign alternative User IDs when necessary to limit the use of Privileged Access. Whenever possible in these situations, Stewards and Custodians shall assign unique User IDs that ensure individual accountability and shall avoid the use of Shared User IDs. Custodians and privileged Users shall ensure that authentication credentials for alternative User IDs are separate and distinct for credentials for normal User IDs. Whenever possible, custodians or other privileged Users shall use their own credentials to access the alternative User ID and shall not know, possess or have access to the Authentication credentials of the alternative User ID.

4. Information Resource Stewards shall review Privileged Access every six months and make any modifications to access or remove access as necessary to comply with this standard.

5. Information Resource Stewards and supervisors shall work with Information Technology Services to ensure that applicants for Privileged Access possess the knowledge, skills, and competencies commensurate with the duties of the position.

6. Information Resource Stewards, supervisors, and Information Technology Services shall review the knowledge, skills, and competencies required for each position with Privileged Access at least annually and shall require additional training, education, or professional development as needed.

7. Information Resource Stewards shall follow all the requirements in preceding sections as they apply to Privileged Access.

8. Information Resource Custodians shall create, modify and retire User IDs and modify Privileged Access only following the approval of the appropriate Information Resource Steward. Custodians shall ensure that these actions are not undertaken without the approval of the appropriate Information Resource Steward.

9. Information Resource Custodians shall control default accounts in applications, systems and services, and shall disable them whenever possible. In cases where use of these accounts is necessary, custodians shall secure these accounts, ensure the default password for said account is changed, and limit their use to employees or affiliates authorized by the appropriate Information Resource Steward.

10. Information Resource Custodians and other Users with Privileged Access shall use a secure process for managing, storing, changing, and accessing authentication credentials associated with Privileged Access. Custodians and Privileged Users shall follow the requirements for Shared User ID authentication credentials listed above.

11. Information Resource Custodians and other Users with Privileged Access shall use the minimum access privileges required while completing tasks. Custodians and Users shall elevate to Privileged Access only when said access is required to complete specific tasks

associated with their duties and shall de-elevate from Privileged Access as soon as these tasks are complete.

12. Information Resource Custodians shall follow all the requirements in preceding sections as they apply to Privileged Access.

13. Information Resource Stewards and Custodians shall maintain a record of all Privileged Access approvals and provisioning actions for review during information security assessments or audits.

14. Supervisors shall notify and work with the appropriate Information Resource Steward and Information Technology Services to address any performance issues related to Privileged Access of Information Resource Custodians or other Users.

15. Supervisors shall follow all the requirements in preceding sections as they apply to Privileged Access.

H. Physical Access Control – Information Resource Stewards shall ensure that the level of Physical Access Control for any area that houses Information Resources is commensurate with the level of risk associated with the loss or compromise of those resources.

1. Data Centers – These locations house enterprise or departmental computing and networking resources and must be secure, safe and stable environments. The appropriate Information Resource Trustee shall assign management and oversight of each data center to an Information Resource Steward. The steward shall ensure that the following requirements are met:

1.1. Information Resource Stewards shall ensure that access is limited to employees or affiliates based on the Principle of Least Privilege in order to protect the physical resources and data from unauthorized use, accidental or malicious damage, and theft. Stewards shall ensure that emergency response personnel have access to data centers.

1.2. Information Resource Stewards shall ensure that data centers are equipped with all necessary features to ensure the safety of resources and continued operation in the event of failures as specified in the Data Center and Server Room Standard and other related standards.

1.3. Information Resource Stewards with responsibilities for data centers shall implement plans to respond to notifications from data center monitoring systems on a 24 x 7 x 365 basis. Data centers that house applications or systems affecting human health and safety shall include notification of Emergency Management and University Police Department personnel.

2. Telecommunications Rooms – These locations house distributed networking resources and must be secure, safe and stable environments. The Associate Vice Chancellor (AVC)

for Information Technology Services and Deputy Chief Information Officer shall serve as the Information Resource Steward for all telecommunications rooms and shall ensure that the following requirements are met:

2.1. The AVC shall ensure that access to equipment in closets, shared mechanical spaces or janitorial spaces is limited to employees and affiliates based on the Principle of Least Privilege in order to protect physical resources and data from unauthorized use, accidental or malicious damage, and theft. The Associate Vice Chancellor for Facilities and the Chief of Police shall have additional responsibility for approving access for their respective staff members, as specified in the Telecommunications Room and Enclosure Standard.

2.2. The AVC shall ensure that network rooms are equipped with all necessary features to ensure the safety of resources and continued operation in the event of failures as specified in the Telecommunications Room and Enclosure Standard.

3. Server Rooms – These locations house departmental computing resources and must be secure, safe and stable environments. While server rooms have a function similar to data centers, they lack the environmental, monitoring and power systems required for data centers, and their use is discouraged. The appropriate Information Resource Trustee shall assign management and oversight of each server room to an Information Resource Steward. The steward shall ensure that the following requirements are met:

3.1. Information Resource Stewards shall ensure that access is limited to employees or affiliates based on the Principle of Least Privilege in order to protect the physical resources and data from unauthorized use, accidental or malicious damage, and theft. Stewards shall ensure that emergency response personnel have access to server rooms.

3.2. Information Resource Stewards shall ensure that server rooms are not used to house enterprise applications or systems, applications or systems that support human health and safety, applications or systems that house or process CSC data, or applications or systems that support information security or physical security.

4. Physical Security Perimeters and Controls – Some additional locations require physical security due to the sensitive nature of the data, hardware, or software processed or housed in those locations. Examples include research labs that collect or process Confidential, Sensitive, or Controlled Data, locations which store personally identifiable information (PII) or personal health information (PHI), or locations where checks are printed. Information Resource Trustees shall assign management and oversight of each such location to an Information Resource Steward. The steward shall ensure that the following requirements are met for these areas:

4.1. Information Resource Stewards shall ensure that access to secure areas is controlled by an electronic card access system or tightly controlled traditional lock and key system.

4.2. Information Resource Stewards may identify a small number of employees or affiliates whose job duties require frequent access to a secure area or area(s). The steward may grant these personnel authorized access to the location(s). Authorized access need not be logged.

4.3. Information Resource Stewards may grant authorized access on a temporary basis to additional employees or affiliates for the period in which job duties require temporary but frequent access to a secure area. Authorized access of these individuals need not be logged.

4.4. Information Resource Stewards shall ensure that all other entry to secure areas by other personnel is strictly limited to legitimate business need or use, and is logged. Personnel with authorized access shall supervise visits by others. Inspections or tours of facilities for educational purposes are legitimate business uses. Logs may be maintained by electronic card access systems, electronic systems, or paper access logs at entrances to secure areas. Logs shall be retained for a period of at least two years.

4.5. Personnel with authorized access to a secure area shall provide unrestricted access to emergency response personnel for the duration of any emergency situation. Authorized personnel shall first provide access to emergency response personnel, then shall notify their supervisor and the appropriate Information Resource Steward as soon as possible.

4.6. Personnel with authorized access to a secure area shall not loan access cards or keys to other individuals.

4.7. Personnel with authorized access to a secure area shall immediately report the loss or theft of an access card or key to their supervisor and the appropriate Information Resource Steward. Access privileges assigned to lost or stolen cards shall be revoked immediately and will be restored only after the card is located or replaced and is presented to the supervisor. Lost or stolen keys shall require prompt rekeying of the secure area.

5. Server Security – These devices store and process data and provide services to other computing devices. Information Resource Stewards shall ensure that servers are housed in a data center or server room and not located in an office or other area. For the purposes of this standard, servers include any computing equipment that provides services other than those permissible on a user device as defined in the Endpoint Configuration and Security Standard.

6. User Endpoint Security – Users shall keep all devices, including mobile devices, which store CSC data in a physically secure location when the user or other responsible individual is not present.

I. Procurement – In order to ensure that proposed Information Resources have the capability to fulfill the requirements of this standard, Information Resource Stewards, Information Resource Custodians, and Users shall ensure that the following requirements are met:

1. Information Resource Stewards, Custodians and Users shall work with Information Technology Services to determine the capabilities required for proposed applications, systems, or services in order to comply with the requirements of this standard.

2. Information Resource Stewards shall ensure that any new Information Resources under their purview have adequate features and controls to comply with the requirements of this standard before these resources are acquired.

3. Information Resource Stewards, Custodians and Users shall submit all Information Resource purchases to Information Technology Services for review and approval prior to acquisition.

VI. 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.

VII. 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

Approved by the Chancellor

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