New Standard: This standard defines the requirements to manage and secure Data Centers and Server Rooms.

NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

DATA CENTER AND SERVER ROOM

UNIVERSITY STANDARD

I. Purpose

This standard defines the requirements, practices, and technical specifications to manage and secure all Data Centers and Server Rooms owned or operated by North Carolina Agricultural and Technical State University (N.C. A&T), regardless of location, specific purpose, or college or division that operates said facility. This includes requirements to manage physical security of all equipment housed within these locations.

This standard is an extension of the university's Information Security Policy (ISP), Acceptable Use Policy (AUP), and Access Control Standard (ACS), and provides additional technical specifications. All requirements and sanctions of these policies and the ACS apply to this standard. This standard also outlines requirements for compliance with the North Carolina Fire Code as required by the Greensboro Fire Department.

II. Scope

This document includes requirements for management and security of all Data Centers and Server Rooms owned or operated by N.C. A&T, regardless of location, specific purpose, or college or division that operates said facility. Guidelines to ensure resiliency and support business continuity efforts are also included.

The management and security controls for Data Centers or Server Rooms that are owned and managed by third parties to provide services to N.C. A&T shall be consistent with the requirements of this standard. Departments that subscribe to such services shall obtain evidence that the third party is compliant with requirements consistent with this standard.

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. Such exceptions notwithstanding, the Steward(s) and Custodian(s) in conjunction with Information Technology Services shall implement alternative security measures to protect the Data Center, Server Room, equipment, the University's network, and other University information resources. Information Technology Services shall approve the configuration, including all such alternative measures, prior to implementation or connection of any equipment to a N.C. A&T telecommunications network.

III. Definitions

Confidential Data – As defined in the ISP, 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 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.

Data Center – A facility designed to house server, storage, and telecommunications equipment in a secure, safe, and stable environment. Data Centers shall employ environmental management, fire suppression, and monitoring systems to protect equipment and data.

Information Resource Custodian (Custodian) – As defined in the ISP, university employees who have been assigned operational responsibilities for managing Data Centers and Server Rooms in compliance with this standard, including maintaining applicable controls such as data security, physical security, resource inventory, backup and recovery. Updates to the definition in the ISP shall have precedence over the definition in this standard.

Information Resource Steward (Steward) – As defined in the ISP, unit or department leaders with planning and management responsibility for Data Centers and Server Rooms, including authorization of access, assignment of Custodians, and ensuring that Custodians comply with this standard. Updates to the definition in the ISP shall have precedence over the definition in this standard.

Information Resource Trustee (Trustee) – As defined in the ISP, senior university officers (e.g., Vice Chancellors, Vice Provosts, Deans, etc.) who have oversight, policy, and compliance level responsibility for Data Centers and Server Rooms. Updates to the definition in the ISP shall have precedence over the definition in this standard.

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. 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 ISP shall have precedence over the definition in this standard.

Server Room – A facility designed to house server, storage, and telecommunications equipment that lacks the environmental management, fire suppression, and monitoring systems found in Data Centers.

IV. Responsibilities

A. Trustees – Trustees are ultimately responsible for the management, security, and integrity of Data Centers and Server Rooms under their purview. Trustees shall assign a Steward to manage their Data Centers or Server Rooms and shall ensure that the requirements of this standard are met.

B. Stewards – Stewards are responsible for the management, security, and integrity of Data Centers and Server Rooms assigned to them by a Trustee. Stewards shall assign Custodians, approve access of Custodians, ensure that Custodians comply with this standard, maintain records, and provide information to ITS as needed.

C. Custodians –Custodians are responsible for the operation of Data Centers and Server Rooms assigned to them by a Steward. Custodians shall ensure that all equipment is installed properly, that facilities and cabling are secured and kept in a clean and organized manner, and shall respond to issues in a timely manner. Responsibilities include maintaining applicable controls such as data security, physical security, resource inventory, backup and recovery. Custodians shall ensure that environmental control, fire suppression, power, and monitoring systems are installed and configured properly, inspected and tested routinely, and maintained in an operating order.

V. Requirements

Data Centers and Server Rooms shall be secure areas as described in the University’s Information Security Policy IV. D. 6., and the Access Control Standard V. H. 1. and V. H. 3.

Moreover, section V.H.5. of the Access Control Standard requires that servers and associated equipment shall be housed in a Data Center or Server Room.

Data Centers house enterprise or departmental computing and networking resources and shall be kept in a secure, safe and stable condition. Data Centers may be used to house enterprise or departmental applications or systems, or applications or systems that support human health and safety, house or process Confidential, Sensitive, or Controlled Data, or support information security or physical security. Server Rooms shall not be used for these purposes but may house Public Data or instructional systems at a departmental level.

In the requirements below, the term Data Center is inclusive of Data Centers and Server Rooms. Specific alternative requirements for Server Rooms are noted as they apply.

A. Access Control and Security

1. Data Centers are secure locations as described in the Information Security Policy IV. D. 6. and the Access Control Standard V. H. 1 and V. H. 3. All requirements of access control and physical security specified in these documents apply to all Data Centers.

2. The appropriate Steward shall authorize access to Data Centers. Authorization shall be guided by the principle of least privilege described in the Access Control Standard. The Steward shall grant access only to those staff members with legitimate duties in a Data Center. Stewards shall maintain records of access authorization for the duration of the authorization assignment and for two (2) subsequent fiscal years.

3. Data Centers shall employ video surveillance systems for perimeter and internal spaces. Video data shall be maintained for ten (10) business days.

4. Data Centers shall be locked at all times unless a staff member with authorized access is working in the immediate vicinity and maintains observation of the Data Center.

5. Data Centers shall have no windows whenever possible. All windows, whether facing the exterior or interior of the building, shall be reinforced and secured to prevent access by unauthorized persons.

6. Employees or contractors shall provide the appropriate Steward or Custodian timely notification of any issues that lack compliance with this standard or otherwise compromise the safety or security of a Data Center.

7. Data Center access shall be monitored and recorded. The appropriate Steward shall maintain access records for two (2) subsequent fiscal years.

B. Operation

1. Data Center equipment designed to be housed in racks or cabinets shall be properly mounted and secured. Equipment designed to be free standing shall be located in areas where there is no danger of the equipment falling or being knocked over. Whenever possible, all racks and free-standing equipment shall be installed with appropriate anti-tip

brackets. Equipment shall be accessible and shall not be obstructed by other equipment or supplies. A clear space with a width of three (3) feet or more shall be maintained around all equipment racks. A clear path with a width of three (3) feet or more shall be maintained from the equipment rack to the nearest door.

2. All items stored in a Data Center shall be kept orderly, tidy, and generally organized. Supplies or small equipment shall be stored on shelving units whenever feasible. All such shelving units shall be properly attached to walls providing the structural integrity necessary so as not to tip, fall, or otherwise cause the stored items to fall onto equipment.

3. No shelving unit shall be erected that will cause, in the event of a failure of said unit, items to fall into or on servers, storage, or telecommunications equipment, or cabinets and racks.

C. Environmental Control and Safety

1. Data Centers shall be equipped with environmental control systems, including air conditioning and humidity control. Whenever feasible, data centers shall be equipped with redundant environmental control systems to ensure business continuity. Server Rooms shall be equipped with environmental control systems if necessary to comply with the following temperature and humidity requirements.

2. Temperature in each Data Center shall be maintained at a maximum of 80 degrees Fahrenheit.

3. Humidity in each Data Center shall be maintained at a relative humidity between 40% and 60%.

4. Data Centers shall employ a monitoring system to alert the appropriate Custodians when the temperature or relative humidity of any room exceeds the level established above. Monitoring systems shall alert Emergency Management and University Police in addition to Custodians of any issues in a Data Center that houses applications or systems affecting human health and safety. Server Rooms may employ a monitoring system at the discretion of the Trustee or Steward.

5. Stewards and Custodians shall develop, maintain and periodically test a plan to respond to issues identified by Data Center monitoring systems. Such plans will provide for 24x7x365 response. Stewards shall maintain records of testing for two subsequent (2) fiscal years. Trustees or Stewards shall determine the response requirements of Server Rooms.

6. Data Centers shall be maintained free from rust, water, dirt, trash, debris, flammable materials, and other contaminates.

7. Data Centers shall be designed with firewalls to protect equipment from external fires and to ensure a contained space for gaseous fire suppression systems.

8. All penetrations of a firewall shall be filled with properly installed fire barrier material rated for two (2) hours or longer of fire resistance, in accordance with the North Carolina Fire Code.

9. Data Centers shall be equipped with a gaseous fire suppression system capable of extinguishing a fire within the Data Center. Gaseous fire suppression systems shall be designed to trigger before sprinkler systems. Fire suppression systems shall be inspected periodically and maintained in proper working order. Server Rooms may be equipped with a gaseous fire suppression at the discretion of the Trustee or Steward.

10. Whenever feasible, Data Centers shall employ dry pipe sprinkler systems.

11. Data Centers shall have no water source within the room that is not solely intended for fire suppression. A drip pan shall be properly installed and maintained below all water supplies, drains, or condensation pipes running over the top of a Data Center.

12. Data Centers shall be equipped with a fire extinguisher carrying a class “C” rating specifically intended for electrical fires. Fire extinguishers shall be maintained in proper working order.

13. Data Centers shall not be used to store equipment or supplies that is not intended for the provision of information services or operation of the Data Center.

14. Data Centers shall be equipped with signage that clearly designates the space as a Data Center and prohibits unauthorized access.

15. Data Centers shall be equipped with a current and accurate building evacuation plan.

D. Power and Cabling

1. Data Centers that house applications or systems that support human health and safety, or information or campus security, shall be equipped with a generator for operation during commodity power failure. Where feasible, other Data Centers shall be equipped with a generator as well. Generators shall be capable of supporting the server, storage, telecommunications, environment control, and monitoring systems within the Data Center. Server Rooms may be equipped with generators at the discretion of the Trustee or Steward.

2. Data Centers shall be equipped with an uninterruptable power supply (UPS) system capable of supporting the server, storage, and telecommunications equipment within the Center for at least one (1) hour. UPS systems shall ensure the delivery of clean and uninterrupted power during a change between commodity and generator power. UPS systems shall be inspected and tested on a regular basis, and repaired or replaced as needed. Server Rooms may be equipped with UPS systems at the discretion of the Trustee or Steward.

3. Data Center wiring shall be kept orderly, tidy, and properly dressed following best practices as outlined in the Building Industry Consulting Service International Standard for Installing Commercial Building Telecommunications Cabling.

4. Data Centers shall be equipped with a minimum of two grounding wrist straps. The wrist straps shall be used whenever workers install, remove, or perform any maintenance on equipment.

5. Server, storage, telecommunications, or other equipment shall utilize properly grounded electrical outlets connecting all equipment power to the building power ground or house ground.

6. Equipment cabinets or racks that reside on top of carpet shall be properly grounded by connecting the cabinet or rack directly to the ground connection of the building's power circuit.

E. Inspection

1. The Steward shall ensure inspection of each Data Center for compliance with this standard on a quarterly basis. Additional inspections may be conducted to meet other requirements such as compliance with the North Carolina Fire or Electrical Codes. Inspection records or copies shall be shared with ITS. ITS shall maintain records for two subsequent (2) fiscal years.

VI. Authorization of Telecommunications Room and Enclosure Access

A. Access to Data Centers shall be based on the principle of least access as required in the Access Control Standard sections V. H. 1 and V. H. 3. The Steward shall grant access only to those staff members with legitimate duties in a Data Center.

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

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

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

Approved by the Chancellor

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