Effective: *Draft*
Last Revised: *03/03/2022*

Responsible University Administrator:
Assistant Vice President, Infrastructure Services

Responsible University Office:
Information Technology Services

Standard Contact:
Data Center Management Team
its-datacenter@nebraska.edu

NU-ITS Data Center Standard

Standard Contents

1. Purpose

This Standard is intended to mitigate physical and environmental risks within data centers managed or operated by University of Nebraska Information Technology Services (NU-ITS).

2. Scope

This Standard applies to all data centers managed or operated by University of Nebraska Information Technology Services.

3. Standard Statement

It is the intention of this Standard to establish best practices pertaining to the physical and environmental security of NU-ITS Data Centers. Deviations from the requirements defined herein in the form of exceptions must be approved in advance and in writing by the Chief Information Security Officer ("CISO") as defined in **ITS Policy Exception Standard**. The following subsections outline the NU-ITS Data Center Standard.

4. NU-ITS Data Center Standard

4.1 Authorized Access to Data Centers

Individuals authorized to approve access to data centers will ensure that all individuals entering the designated areas have authorized access. Access will be granted in accordance with the following matrix:

Access Level	ITS Data Center	ITS Colocation Data Center
Authorized to Approve Access	• Data Center Management Team	• Data Center Management Team
Implement Approval	• NU-ITS Infrastructure Services	• NU-ITS Infrastructure Services
Category 1: Fully authorized with card access and is permitted in the facility without restriction to perform essential job functions.	• VP, Information Technology • AVP, Infrastructure Services • Executive Director, Infrastructure Services • Infrastructure Architecture Staff • IT Disaster Mitigation Staff • NU-ITS Network Services Staff • NU-ITS Systems Services Staff • NU-ITS Telecom Services Staff • NU-ITS Information Security Services Staff • NU-ITS Endpoint Services Staff • NU-ITS Operations Center Staff • UPS/CRAC Maintenance Contractor • UNL Police "TBD" • UNL Facilities "TBD"	• AVP, Infrastructure Services • Executive Director, Infrastructure Services • Infrastructure Architecture Staff • IT Disaster Mitigation Services Staff • NU-ITS Network Services Staff • NU-ITS Systems Services Staff
Category 2: NO card access but will be permitted entry on an as-needed basis to perform job functions. Required to sign visitor log but do not have to be escorted.	• Individuals owning equipment within the facility • Vendors • Contractors	• NU-ITS Telecom Services Staff • NU-ITS Information Security Services Staff • Vendors • Contractors
Category 3: NO card access and will only be granted access on a case-by-case basis. Required to sign visitor log and may require escort.	• All others not listed above will be allowed entrance on a case-by-case basis	• All others not listed above will be allowed entrance on a case-by-case basis

Individuals requesting access to any secured location must have a University of Nebraska/State of Nebraska photo ID badge. In the absence of a photo ID, an employer issued photo ID may be an acceptable form of identification. Individuals without appropriate photo identification will not be given access.

4.1.1 NU-ITS Data Center Access Procedures

- Access requests will be submitted through and associated actions tracked within the ITS ticketing system.
- Data center entry and egress doors shall alert the Data Center Management Team when left open in excess of five (5) minutes in order to reduce the risk of unauthorized access.
- Access logs for data center doors will be forwarded to Splunk for retention.
- Access logs will be reviewed by the Manager, Hosting Services quarterly.

4.1.2 NU-ITS Colocation Data Center Access Procedures

- Security and environmental controls for colocation data centers are managed provided by the colocation facility operator.
- Modifications to lists of authorized staff are maintained in accordance with data centers and updated per the colocation facility operator's requirements.
- Access logs for colocation data center doors are stored and reviewed in accordance with the colocation facility operator's requirements.

4.1.2 Removal of Access

In coordination with an individual's manager, access will be removed if an individual has abused access privileges, or if access is no longer required as part of the position requirements.

4.1.3 Tours of Facilities

Tours of data center facilities are only available on a limited basis upon the approval of the Data Center Management Team or their designee. All tours must have a member of Infrastructure Services with Category 1 access in attendance.

4.1.4 Auditing

The Manager, Hosting Services shall review the list of people who have received authorization to data centers at least once per semester. A report of the number of people accessing the area and the number of people removed as a result of the audit shall be provided to the Assistant Vice President, Security & Identify Services.

4.1.5 Access Requirements

Equipment

- All mail, boxes, hardware, and etc. shall be inspected for evidence of tampering and confirmed contents prior to being moved into the data center.
- Packing materials will be disposed of as soon as the contents have been inspected. Floor tiles must be replaced properly, and all floor tile cutouts must be covered. Any opening in the floor at the end of work must be temporarily marked by placing an orange safety cone on at least one side of the opening. All tiles must be properly installed when put back in place; any tiles that have raised edges must be immediately corrected.
- Data center staff will be responsible for all racking of equipment, running of cables, and moving of ports.
- All personnel are to follow safe lifting procedures when performing any lifting tasks.
- Fire extinguishers and emergency exits are not to be blocked at any time.
- Request for data center Installation/Removal/Relocation/Rename must be submitted through the NU-ITS ticketing system for approval by the Data Center Management Team prior to any action being taken.
- Where appropriate, IP-KVM consoles and/or crash carts are available for console access to equipment.

Vendors & Contractors

- Vendors & contractors may not wander around the data center; they should stay near the area where their server is located.
- Vendors & contractors are responsible for disposal of their own trash. Trash is to be placed in identifiable receptacles.
- Vendors & contractors will be escorted or monitored while working within the data center.

Physical Appearance of Data Center

- No materials of any kind shall be left in racks or on top of racks.
- During normal business hours, dress code standards of the organization must be followed.
- Under no circumstances will food or beverages be allowed within Data Centers.
- In instances when prolonged work is required, a work table and chairs may be temporarily setup within the Data Center.
- All individuals who enter the data center are responsible for ensuring the area is kept neat and clean.

4.2 Assets and Property

The University of Nebraska defines assets as equipment acquired at a cost over $5,000. Any equipment meeting this criterion will be tagged with a University asset tag and tracked within SAP. NU-ITS further extends this criterion for the purposes of managing equipment within data centers.

- Any electronic equipment supporting the network, compute, storage, or telephony needs of the University that has an acquisition cost greater than $5,000 will have an RFID asset tag affixed; in addition to the University asset tag. Assets under $5,000 may have an RFID asset tag affixed at the discretion of the Data Center Management Team.
- The following information will be tracked within the RFID asset inventory system and associated with each asset:
    - Manufacturer
    - Model Number
    - Serial Number
    - Acquisition Cost
    - Acquisition Date
    - First Placed in Service Date
    - End of Life (EOL) Date
    - End of Support (EOS) Date
    - Location – Building
    - Location – Room
    - Location – Rack and Elevation
- In addition to the RFID asset inventory system, NU-ITS will maintain a Data Center Floor diagram. The floor diagram, at a minimum, will identify the location of environmental and electrical equipment and controls, data center racks, and physical security controls.
- Authorized staff performing equipment installation must submit an “Installation Request” through the NU-ITS ticketing system.
- Authorized staff performing equipment relocation must submit a “Relocation Form” through the NU-ITS ticketing system.
- Authorized staff performing equipment removal must submit a “Removal Form” through the NU-ITS ticketing system.
- Installation, relocation, and removal ticket reports will be reviewed monthly against the RFID asset inventory system by the Manager, Hosting Services or their designee.
- Equipment installed into the data center must be rack-mountable and housed in standard racks using standard rack configurations. Any exceptions must be approved by the Manager, Hosting Services or their designee prior to installation.
- University equipment must be removed from the data center within 90 days after decommission of services. Any assets containing sensitive, restricted, or regulated data as defined in ITS-05 must be sanitized by physically destroying the drives containing the data. Any other assets should be electronically erased or factory-reset. After sanitization, the assets must be disposed of in accordance with University asset surplus and disposal guidelines.

Inventory of assets will be reviewed annually by the Manager, Hosting Services or their designee. This annual review will include a review of asset movement into and out of the facilities. This review will be conducted in tandem with the Inventory and Accounting inventory review and annual inventory audit processes. This review will include verification of movement of assets within the data center. Reports from the annual and annual asset reviews will be stored in the NU-ITS – Infrastructure Services OneDrive folder structure.

4.3 Environmental Controls

4.3.1 Acceptable Ranges and Desired Setpoints

- Temperature: Average room temperature of 65 – 75 degrees Fahrenheit
- Humidity: Average room humidity of 40 – 60%

4.3.2 Acceptable Ranges and Desired Setpoints

- HVAC
  - Computer Room Air Conditioner (CRAC) Units:
    - Cooling and related equipment must be sized to account for:
      - The size of the cooling load of all equipment.
      - The size of the cooling load of the building (lighting, power equipment, personnel, building envelope).
      - Over sizing to account for humidification efforts.
      - Over sizing to account for redundancy should a unit fail (N+1).
      - Over sizing to account for appropriate future growth projections.
    - All cooling equipment must be designed, installed, and maintained by qualified technicians that meet state and local codes. All cooling equipment must follow the manufacturer's recommended maintenance schedule.
    - Air filtration media should be installed at air intake points. Media should be replaced on a regular schedule based on the manufacturer's recommended filter lifespan.
  - Humidity and temperature controls:
    - Humidity and temperature must be maintained at a level that is compliant with the equipment installed within the data center.
    - Humidity injection units must have separate drains and be fed by conditioned water.
  - Pump systems:
    - Units must be located in a secure room.
    - Units should be designed and installed to eliminate single points of failure.
    - Pumps must restart automatically after a power failure.
    - Pumps must have an emergency power source to allow time for a controlled shutdown of supported areas.
  - Pipe systems:
    - Pipe must be constructed of high-quality rust- and coolant- resistant material.
    - Pipe loops must have valves in several locations that allow sections of the loop to be isolated without interruption to the rest of the loop.
    - Pipe loops must have isolation valves for each CRAC unit.
  - Air delivery management:
    - Cold air delivery must be managed such that the required amount of air can be delivered to any necessary equipment location.
  - System monitoring:
    - All infrastructure systems supporting data centers must be monitored on a continual basis.
    - Monitoring must be available at a central location such as the Operations Center.
    - Monitoring system must support a master reporting console that can also be accessed remotely (including history logs) and must notify support staff of alarms at central and remote sites.
    - Water detection must be present around CRAC units and at the lowest point of the room.
- Electrical Systems
  - Main and step-down transformers:
    - Must be located in a secure mechanical room.
    - Must have HVAC systems to support heat load and correct humidity levels for each unit.
    - Must be maintained by a qualified technician to factory standards and be supportable by extended factory warranty.
  - Main power control panel and Program Logic Control (PLC):
    - Must be maintained by a qualified technician to factory standards.
    - Must be located in a secure mechanical room.
    - Must have HVAC systems to support heat load and correct humidity levels for each unit.
    - Must have surge suppression sufficient to prevent large surges from damaging panels and equipment supported by the panel.
    - PLC must have password security.
    - PLC must have UPS support for power failure.
  - Motor control panels:
    - All controls must have automatic restart after power failure.
    - Must be maintained by a qualified technical to factory standards.
    - Must be located in a secure mechanical room.
    - Must have HVAC systems to support heat load and correct humidity levels for each unit.

- UPS systems:
  - UPS systems in the data center must be sized to meet current and future needs, with sufficient battery backup to allow for a controlled shutdown of primary servers.
  - UPS systems must be designed, installed, and maintained by authorized electricians and technicians and housed in a secure location.
  - UPS systems must follow manufacturer's recommended maintenance schedule.
  - UPS systems must have bypass capability to allow for periodic maintenance.
- Backup batteries:
  - Must follow manufacturer's recommendations for system to be of sufficient quality and capacity to ensure a long life thus limiting breaks in the battery strings.
  - Must be located in secure area with proper ventilation as required.
  - Must be installed and maintained by authorized technicians.
  - Must be approved for use in computer equipment UPS systems.
- Sub-panels:
  - Must be sized to meet current and future needs.
  - Must be located in the data center to minimize power runs to desired equipment.
  - Panel maps must be maintained to reflect their most current usage.
  - Sub-panels must never be opened at the face plate by anyone other than qualified electricians.
  - All materials must be at least three feet away from sub-panels.
- Remote Power Panel (RPP) units:
  - Must be located to maximize ease of distribution to equipment.
  - Must comply with BS/IEC/EN 60439-1.
- Power strips:
  - Must be sized to meet the power requirements of the cabinet in which they are installed.
  - Power receptacles for power strips must be installed by authorized electricians.
  - Monitoring systems must be IP capable.
- Power cable layout:
  - The power pathways must maintain a minimum separation from data cable pathways in accordance with ANSI/TIA-469-B Standards and the University of Nebraska Design and Construction Standards Division 27 for Telecommunication Systems.
  - Equipment power cables should be the minimum required length and slack/strain management must be employed.
  - Cables must be arranged to minimize airflow disruptions.
- Grounding systems:
  - All data center equipment must be grounded in compliance with state and local codes.
  - Data center equipment grounds must be independent of all other building grounds (such as lightning protection systems).
  - All metal objects must be bonded to ground, including cabinets, racks, PDUs, CRACs, cable pathway, and any raised floor systems.
  - Ground resistance should be < 1 Ohm.
- Monitoring system:
  - All electrical equipment must be monitored.
  - Monitoring systems must be IP capable.
  - System must have a central monitoring console located in an area such as a NOC and be remotely accessible.
  - System must be able to report alarms at the central and remote consoles by email and send recorded cell phone messages.
  - Monitoring system must have analysis and reporting function.
  - System must be able to retain log files of equipment performance and incident history.
- Generator management:
  - Generators must be start tested and run for at least one hour once per month.
  - A full load test and switching test must be conducted at least once per year.
  - Maintenance logs must be kept on all tests and reflect maintenance performed.
  - All maintenance must be performed by a qualified technician to factory standards.
  - Management must include a remote alarm panel (enunciator panel).
- Maintenance and testing:
  - All electrical system components should be regularly inspected.
  - Main power switches, transformers, automatic transfer switches, and other major electrical system equipment must be maintained by qualified technicians per factory specifications and recommendations for service cycles.
  - Reports from regular inspections must be provided to the Manager, Hosting Services or their designee for review.

- Fire alarm and suppression systems
    - Suppression systems must be designed specifically for use in data centers.
    - Suppression systems must comply with all state and local building codes.
    - Suppression systems must use chemicals that do not damage sensitive equipment.
    - Suppression systems must not pose harm to building occupants.
    - Suppression systems must be maintained by qualified technicians to factory standards.
    - Reports from regular inspections must be provided to the Manager, Hosting Services or their designee for review.
- Raised floor systems
    - Under floor space management:
        - Must remain clear and corrosion free.
        - Constant air pressure must be maintained at all times.
        - Must remain obstruction free for proper air flow.
    - Cleaning:
        - Must be done with a vacuum cleaner equipped with HEPA/S-class filters.
        - Must be done on a continual basis.
    - Floor structure maintenance:
        - Must be corrosion and rust free.
        - Damaged pedestals, cross-members, tiles, or missing fasteners must be replaced immediately to maintain floor integrity.
    - Floor grounding:
        - Must be separate from building ground.
        - Must comply with all state and local codes.
- Server Cabinet Systems:
    - Cabinet standards:
        - Data center rack enclosures must have 42U vendor neutral mounting rails that are fully adjustable and compatible with all EIA-310 (Electrical Industry Alliance Standards) compliant 19” equipment.
        - Cabinets must have access points for power and data pathways at the top and bottom of the cabinet.
        - The data center site must have a standardized set of cabinets tailored to the site’s specific needs.
    - Cabinet layout:
        - The cabinets will be configured in a standard hot aisle cold aisle configuration.
        - The cold aisle edge of the equipment enclosures must line up with the edge of the floor tiles.
        - Hot and cold aisles must be wide enough to insure adequate access to equipment and safe staff workspace.
        - In cases where vented floor tiles alone are insufficient to heat load for an area, additional cooling measures will be used.
        - Blanking panels will be installed in any unused rack space to minimize cold/hot air mixing.
    - Cabinet security:
        - All cabinets must be lockable.
        - All cabinets must reside in a secure area within the data center.
    - Cabinet loading:
        - Rack loading must not exceed the weight rated capacity for the location’s raised floor.
        - Rack heat load must not exceed the cooling capacity of the location.
        - Large servers and equipment must be installed at the bottom of the rack.
- Cable Plant
    - Overhead delivery system cable layout:
        - The data center must have a system to support overhead delivery of data connections to the equipment cabinets.
        - The data pathways must maintain a minimum separation from high voltage power and lighting in accordance with ANSI/TIA-469-B Standards (American National Standards Institute/Telecommunications Industry Association) and the University of Nebraska Design and Construction Standards Division 27 for Telecommunication Systems.
    - Fiber standards:
        - Fiber installation must use 50 micron OM3 laser optimized fiber or better, rated for the capacity of the connection.
        - All fiber installations must be labeled and comply with the NU-ITS Labeling Standard.

- Copper standards:
  - Copper jumpers must be CAT5E or newer with RJ45 connectors, rated for the capacity of the connection.
  - All copper data cables must be labeled and comply with the NU-ITS Labeling Standard.
- Grounding:
  - All cabinets and cable delivery pathways must be grounded in compliance with the University of Nebraska Design and Construction Standards Division 27 for Telecommunications.

4.3.3 Support Services

- Server Installation
  - Power:
    - Systems with redundant power supplies must have their power cords plugged into separate power strips.
    - Power must be isolated from data cables.
    - Power cords must be factory certified.
    - Power cords must be clearly labeled and comply with the NU-ITS Labeling Standard.
  - Rack space:
    - Servers must be installed from the bottom up in the rack enclosures.
    - Equipment must be clearly labeled and comply with the NU-ITS Labeling Standard.
  - Data connections:
    - Cable must not exceed required length by more than one foot.
    - Must be isolated from the system and rack power delivery system.
    - Must be clearly labeled and comply with the NU-ITS Labeling Standard.
  - Fiber connections:
    - Fiber must not exceed required length by more than one meter, after service loop is installed per University of Nebraska Design and Construction Standards Division 27 for Telecommunications.
    - Must be clearly labeled and comply with the NU-ITS Labeling Standard.
    - Must not exceed minimum bend radius as specified by the manufacturer.
- Network layout
  - Standard switch layout:
    - All University networking equipment must be approved by NU-ITS network staff and installed by them or their designee regardless of ownership.
    - Switches must be installed in a fashion to minimize the length of data cables required to provision a data connection.
  - Highly critical system switch layout and redundancy:
    - In the case of a highly critical system where network path redundancy is required, the systems must have redundant data circuits that connect to separate switches.
    - Redundant switches must be plugged into separate power strips.

4.3.4 Data Center Risk Management

- NU-ITS shall conduct an annual risk assessment on the physical and environmental controls to ensure they continue to mitigate risk to an acceptable level. These risk assessments shall be coordinated by the Manager, IT Disaster Mitigation and stored in the NU-ITS – Infrastructure OneDrive folder structure.
- NU-ITS shall maintain a Disaster Recovery Plan for data center facilities. Disaster Recovery Plans specific to individual services operated within the facilities are the responsibility of the owner of the service. NU-ITS disaster recovery planning will be coordinated by the Manager, IT Disaster Mitigation and stored in the NU-ITS – Infrastructure OneDrive folder structure.
- NU-ITS shall test data center facility disaster recovery plans at least once per year and/or after a significant change to the data center environment has occurred. These disaster recovery plan tests will be coordinated by the Manager, IT Disaster Mitigation and stored in the NU-ITS – Infrastructure OneDrive folder structure.
- Any service impacting or information security incident related to or within NU-ITS data centers will trigger the ITS Incident Management Plan.

5. Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.

6. Compliance

Compliance Measurement
The University of Nebraska NU-ITS Infrastructure Services team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Standard owner.

Exceptions
Any exception to the Standard must be documented and formally approved by the CISO. Standard exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the Standard exception is required
- Any risks created by the Standard exception
- Risk mitigation plan and duration of the exception
- Evidence of approval following established Exception Standard

Non-Compliance
Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

8. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:		AVP for Infrastructure Services	
Approved by:		VP for IT	
Authorized by:		University President	

Revision history of this Standard:

Version	Date	Description
1.0	03/03/2022	Initial Standard Drafted