INFORMATION TECHNOLOGY SERVICES
George Mason University

Data Center Physical, Environmental & Operational Controls Center Standard

Document Version Number:	1.6
Document Control Number:	ITS.EIS-STD004
Last Updated:	9/26/2025
FOIA Exempt?	No

Process Owner:

- ITS Enterprise Infrastructure Services – Facilities & Infrastructure Operations

PURPOSE:

The purpose of this standard is to define the requirements for physical, environmental, and operational controls to ensure that both Aquia Data Center ("data center") and Disaster Recovery (DR) Site remain professional, state-of-the-art, clean, reliable, safe, and secure. The corresponding control descriptions from NIST SP 800-53 are referenced in brackets at the end of each standard.

Relevant IT Security Control Families:

- CP-06: Alternate Storage Site
- CP-06(1): Alternate Storage Site | Separation from Primary Site
- CP-07: Alternate Processing Site
- CP-07(1): Alternate Processing Site | Separation from Primary Site
- CP-07(4): Alternate Processing Site | Preparation for Use
- PE-01: Policy and Procedures
- PE-06(1): Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment
- PE-06(3): Monitoring Physical Access | Video Surveillance
- PE-08: Visitor Access Records
- PE-09: Power Equipment and Cabling
- PE-09(2): Power Equipment and Cabling | Automatic Voltage Controls
- PE-10: Emergency Shutoff
- PE-11: Emergency Power
- PE-11(2): Emergency Power | Alternate Power Supply, Self-Contained
- PE-12: Emergency Lighting
- PE-13: Fire Protection
- PE-13(1): Fire Protection | Detection Systems, Automatic Activation and Notification
- PE-13(2): Fire Protection | Suppression Systems, Automatic Activation and Notification
- PE-14: Environmental Controls
- PE-14(1): Environmental Controls | Automatic Controls
- PE-14(2): Environmental Controls | Monitoring with Alarms and Notifications
- PE-15: Water Damage Protection
- PE-15(1): Water Damage Protection | Automation Support
- PE-16: Delivery and Removal
- PE-17: Alternate Work Site

Titles and department names are subject to organizational changes.

SCOPE:

This standard applies to all authorized Information Technology Services (ITS) employees, various authorized departmental employees who use the data center services, and authorized business partners of ITS, including contractors, vendors, and other authorized state agency employees.

RESPONSIBILITIES:

Each role performs functions as outlined in the Requirements section:

- ITS Facilities & Infrastructure Operations (FIOPS) Manager
- ITS FIOPS Staff / Operator
- University Facilities Management Personnel
- ITS Facilities & Infrastructure Engineering (FIENG) Manager
- ITS Network & Security Engineering (NSENG)
- Card Access Security Office (CASO)
- Executive Director of ITS Enterprise Infrastructure Services (EIS)
- IT Security Office Director
- ITS Human Resource Liaison
- Colocation Administrators

REQUIREMENTS:

1. Accessibility
    a. The approving authorities for access to the data center and the DR site are the ITS Facilities & Infrastructure Operations (FIOPS) Manager, Executive Director of ITS Enterprise Infrastructure Services (EIS), and Vice President and Chief Information Officer, ITS. [PE-2(a), PE-2(b)]
    b. Access to the data center and DR Site must be restricted to authorized university staff.
    c. Vendor access: Authorized ITS personnel must check the vendor's credentials before allowing him/her inside the DR Site, where he/she will remain with the vendor at all times. [PE-3(a.2)]
    d. Authorized personnel must only enter the data center and DR Site to perform tasks that cannot be performed remotely.
    e. Badge access for both the data center and DR Site is for authorized personnel only. [PE-3(a.1.), PE-3(a.2)]
    f. Vendors, visitors, authorized colocation customers, and non-authorized ITS staff must show proper identification to the FIOPS Manager or Operator on Duty before entering the data center. [PE-3(a.2)]
    g. Vendors, visitors, authorized colocation customers, and non-authorized ITS staff must sign in/sign out on the visitor guest log at the data center. [PE-3(a.1), (PE-3(a.2), PE-3(b)]
    h. Visitors, vendors, and non-authorized ITS staff must be escorted at all times in the data center by authorized personnel. [PE-3(d)]
    i. The master key to the data center and DR Site shall be kept by the university police department. [PE-3(e)]
    j. All contractors hired to perform work in the data center and DR Site must coordinate their work with the FIOPS Manager or Operator on Duty.

Titles and department names are subject to organizational changes.

k. Individuals who no longer require access to the data center and DR Site must be removed from the authorized list and access revoked immediately by the FIOPS Manager or Operator on Duty upon receipt of a request from the individual's group manager. [PE-2(d)]
l. In cases where ID badges are lost or misplaced, old ID badges must be disabled, and new ID badges and PINs must be created. [PE-3(g)]
m. The University Facilities Management personnel are responsible for the generator's security. [PE-3]

2. Monitoring Physical Access
    a. FIOPS must control physical access to publicly accessible areas in both the data center and DR Site through the use of surveillance camera(s), card reader(s), and physical structures (doors). [PE-3(c)].
    b. FIOPS shall control physical access to system distribution and transmission lines in the data center by using cable trays. [PE-4]
    c. FIOPS must monitor physical access to the data center and DR Site through the use of access logs and surveillance camera(s). [PE-6(a), PE-6(1)]
3. Environmental Controls
    a. Power cables in the data center shall be protected by a rigid or flexible metal conduit to prevent damage and destruction. [PE-9]
    b. Emergency power switches shall be located in the data center to provide safe and easy access for FIOPS personnel. [PE-10 (b)]. These emergency power switches shall be used to turn off power in emergency situations. [PE-10(a)]. Emergency power switches must be protected against unauthorized activation. [PE-10(c)]
    c. Auxiliary Power, such as UPS units, provides a short-term uninterruptible power supply to facilitate orderly shutdown of systems in the event of electrical power loss. [PE-11] A dedicated back-up generator provides power to the data center to the limit of its diesel fuel supply. [PE-11(1)]
    d. The emergency lighting at the exit and evacuation routes remains on at all times regardless of the event of electrical power loss. [PE-12]
    e. Fire suppression and detection systems shall be automatic and supported by an independent energy source. These systems are activated automatically, and the fire department is notified in the event of fire. [PE-13, PE-13(1), PE-13(2), PE-13(3)]
    f. Redundant air handlers shall be used should one fail in order to maintain proper temperature (air conditioning) and humidity levels in the data center.
    g. Both the master water shut-off valve and water shut-off valves on HVAC units help minimize water damage to the information systems in the data center. Key ITS FIOPS personnel must be aware of their locations. Only authorized personnel, such as University Facilities Management Personnel, may open or close these water valves. [PE-15]
4. Environmental Monitoring
    a. The FIOPS Manager or Operator on Duty shall use an ITS-approved data center infrastructure management software to monitor and control temperature, relative humidity, and dew points in the data center and DR Site. [PE-14(b)].
    b. 40-ft Leak Rope Sensors running along the left, right, and center of the data center's floor shall detect the presence of water in the data center.
    c. Monitors shall be physically connected to all Heating, Ventilation, and Air Condition (HVAC) units, PDUs, and UPS units in both the data center and DR Site.
    d. FIOPS personnel are required to make physical checks of the data center twice during an 8-hour shift and log or escalate any abnormal conditions; Incidents are recorded in the daily status log; serious environmental conditions are reported immediately to University Facilities Management Personnel for appropriate action and/or repairs.
5. Safety

a. If work is being performed or a floor tile is removed, safety cones must be used around any area left unattended.
b. All rack/computer cabinets and doors must remain closed at all times (when not being serviced).
c. All modifications to the electrical service must be performed by university electricians or an authorized contractor. All such changes must be coordinated with the FIOPS Manager for submission of the required work order(s).
d. No work will be done below the raised floor area without the notification of the FIOPS Manager or Operator on Duty.
e. No industrial cleaning liquids/fluids will be left in the data center unattended.
f. No highly ammoniated or chlorinated products shall be allowed in the data center.
g. No food or drinks are allowed on the main data center floor.
h. The entry doors to the data center must remain closed and locked at all times.
i. Authorized persons entering or leaving the data center must verify that access doors are closed securely to prevent unauthorized persons from entering or tailgating into the area. [PE-3(a.2)]
j. No boxed or loose equipment or other related materials are to be stored on the main data center floor.
k. PDU cabinet panels should not be opened except by the FIOPS Manager in the event of updating the circuit breaker listing or turning the circuit breakers off.

6. Air Quality
   a. The relative humidity and temperature levels must be maintained at recommended and acceptable levels defined by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE) guidelines. [PE-14(a)]
   b. No floor tiles shall be removed, other than temporarily, as this creates unbalanced airflow. No additional vents, grilles, or perforated tiles will be added without coordination with the FIOPS Manager.
   c. Because of the need to maintain sub-floor air pressure in the data center, the number of tiles pulled must be kept to a minimum. All vented floor tiles must be returned to the position from which they were removed.
   d. All tile alterations must be reviewed, approved, and coordinated with the FIOPS Manager. If holes must be cut in the floor panels to accommodate new equipment, the panel shall be removed from the data center to cut the hole. The FIOPS Manager will assist with any floor tile alterations needed.
7. Equipment
   a. HVAC Systems
      i. No changes shall be made to the data center HVAC systems without consultation and approval of the FIOPS Manager.
      ii. University Facilities Management Personnel coordinate and manage all maintenance activities for the HVAC systems, coordinating the work with the FIOPS Manager.
   b. ITS Production Systems
      i. All modifications to production hardware systems must be scheduled whenever possible, following the change management process and procedures, and coordinated with the FIOPS Manager.
      ii. All changes in location, deletions, or additions of equipment must be coordinated with the FIOPS Manager.
      iii. No hardware, racks, furniture, shelving, or other materials will be removed or added without coordinating it with the FIOPS Manager.
      iv. All equipment must be rack-mountable. Exceptions must be reviewed and approved by the FIOPS Manager.

v. All open slots within racks must be closed with blanking panels mounted on the front side of the rack at the data center.
vi. Labeling will be provided on the outside of racks displaying rack location and electrical circuit information. Any changes that affect the accuracy of this information must be provided to the FIOPS Manager, and all labels must be updated.
vii. All significant changes within the data center and DR Site are subject to review, approval, and documentation by the change management process and the FIOPS Manager.
viii. All space allocations are the responsibility of the FIOPS Manager. All projects requiring additional rack space must be coordinated with the FIOPS Manager.

c. Decommissioned IT Equipment
   i. Equipment owners are responsible for the decommissioning of their equipment in the data center. All removal of decommissioned equipment must be coordinated with the FIOPS Manager and Operator on Duty for proper documentation of data center assets and for security purposes via email and the ticketing system. [PE-16]
   ii. All decommissioned equipment must be powered off and removed as soon as possible.
   iii. All decommissioned cabling, including voice, data, and fiber, must be removed as soon as possible.
   iv. When equipment is removed from the data center and DR Site, all pertinent documentation must be updated. This includes asset management, CMDB, and any support matrix that references decommissioned equipment. [PE-16]
d. New IT Equipment
   i. All equipment deliveries must be coordinated with the FIOPS Manager or Operator on Duty to ensure proper receipt, storage, and documentation. Each group/unit will be responsible for notification and/or acceptance of equipment. [PE-16]
   ii. To ensure appropriate use of data center space, placement of new racks must be coordinated by the FIOPS Manager.
   iii. New equipment must be unpacked at the staging/storage area adjacent to the data center prior to its placement in the data center environment.
   iv. Equipment owners are responsible for the installation of their equipment in the data center. All installations must be coordinated with the FIOPS Manager via email and the ticketing system. After the installation, all tools and materials must be removed from the data center floor, and the area must be free of any trash or debris.
   v. ITS Network & Security Engineering (NSENG) staff manage the connectivity requirements, and ITS Facilities & Infrastructure Engineering (FIENG) installs data/telecommunications cabling in the overhead conveyance system (wiring tray).
   vi. All cable runs must run in an orderly manner and be dressed out for a professional appearance. No cables should run diagonally in the sub-floor without prior approval. Electrical and computer cables must run perpendicularly. When cables cross paths, they must be in a perpendicular manner.
   vii. All cabling within racks shall be neatly organized and tied appropriately, allowing rack doors to close.
   viii. No other cabling or material must be used in the tray system without prior approval of the ITS FIENG Manager.
e. Electrical Power
   i. Power requirements for equipment must be provided to the FIOPS Manager before installation. The FIOPS Manager will verify the availability of power and coordinate the documentation of the equipment location and power requirements in the data center layout.

ii. Only qualified University Facilities Management personnel shall open or change any power panel or PDU.
iii. Only the PDUs located in the equipment racks shall be used to provide power for racked equipment. Exceptions: In case of emergency installations, where equipment must be brought into service before a permanent power source can be installed. If used in this manner, a temporary power strip must be tagged and dated. Plans for permanent power must be made with the FIOPS Manager.
iv. PDUs located in equipment racks must not be used to power cleaning equipment or tools. These cleaning equipment/tools must only be plugged into wall outlets located on the outer walls around the data center. Data center staff will provide extension cords or power strips if requested.
v. No non-computer-related equipment should be plugged into any dedicated circuit or PDUs.
vi. Modifications in the data center power design and/or the addition of power outlets must be coordinated with the FIOPS Manager for installation.
vii. The University Facilities Management Personnel is responsible for the generator's maintenance.

f. Other Items
i. All furniture (e.g., desks, chairs, tables, racks, and cabinets) must not be removed from the data center without the consent of the FIOPS Manager.
ii. Use of the Genie Lift must be coordinated with the FIOPS Manager or Operator on Duty.
iii. Only authorized personnel shall access output devices (e.g., printers or copiers) in the data center. [PE-5]
iv. Colocation customers must coordinate with the FIOPS Manager when adding their hardware equipment in the data center. Colocation customers must start adding their equipment from the bottom of the racks.
v. All system racks within the data center must always remain locked unless approved by the FIOPS Manager or Operator on Duty, or pre-approved services are being performed.
vi. Keys will be controlled and maintained by data center operations for all system racks within the data center environment.
vii. Any individual requiring access to their identified systems racks within the data center must be accompanied by the Operator on Duty to the systems rack, which shall be unlocked by the data center Operator on Duty.
viii. Upon completion of services within the individual systems racks requiring access, the data center Operator on Duty must re-lock the systems rack.
ix. Access doors and card readers to the data center are maintained by the Card Access Security Office (CASO).

8. Labeling
a. All equipment must be labeled on the front and rear panels with identification information.
b. All equipment must have a label affixed identifying the PDU and the main power panel to which it is attached.
c. Labeling on the outside racks must display rack location and electrical circuit information.

9. Reporting and Review
a. FIOPS must maintain a list of individuals with authorized access to both the data center and the DR Site. [PE-2(a), PE-3(b)]
b. The FIOPS Manager must maintain hard copies of signed data center access forms for individuals who have been approved for access to the data center. [PE-2(a)]

c. FIOPS must maintain a visitor guest log at the entry/exit points of the data center. [PE-3(b), PE-8(a)] The visitor guest log must be archived for no less than (2) years for audit (external) review purposes before being properly disposed of.
d. The FIOPS Manager must review a list of all individuals having access to the data center and DR Site every quarter to verify that only authorized personnel have been granted access. Continued access for an individual requires positive confirmation from that individual's departmental authority that access is still required. [PE-2(c)]
e. The IT Security Office Director and ITS Human Resource Liaison must review and verify a list of all individuals with access to the data center and DR Site on a semi-annual basis to ensure that any names on this list that have been identified as being separated from Mason or ITS will have their access removed. [PE-2(c)]
f. Colocation Administrators must review a list of their colocation students who have current access to the data center on a semi-annual basis to verify that only authorized students have been granted access. [PE-2(c)]
g. The FIOPS Manager, Executive Director of ITS Enterprise Infrastructure Services (EIS), and IT Security Office Director must review the Swipe-card Usage Logs at both the data center and the DR Site on a semi-monthly basis to spot check for i) suspicious or inappropriate access activity, and ii) time lapse. [PE-2(c)] Any questionable use of access must be investigated and reported to the appropriate personnel to resolve security incidents. [PE-6(c)] Any period exceeding (6) six months (183 days) shall be reported to the cardholder's supervisor, questioning the need to maintain access.
h. The FIOPS Manager must review the Aquia Data Center Visitor Guest Logs monthly. [PE-2(c), PE-8(b)] Auditing visitor guest logs helps identify individual accountability, reconstruct events, and provide evidence of possible violations.
i. The FIOPS Manager must review the list of trusted vendors monthly to monitor their need for access. [PE-2(c)]
j. FIOPS must inventory card readers, keys, and combination locks in the data center on a semi-annual basis. [PE-3(f)]

10. Alternate Work Site
    a. ITS personnel must comply with University Policies (UP) #1114, 1311, and 2202 when teleworking or working from remote sites. [PE-17(a)]
    b. The SciTech Data Center in Prince William shall be the failover site in cases where the Aquia Data Center is no longer functional or secured. [PE-17(a)]
    c. ITS Personnel must comply with UP #1305, Reporting Electronic Security Incidents, in cases of security incidents or problems. [PE-17(c)]

COMPLIANCE:

To ensure compliance with the standards through monitoring and enforcement:

- Compliance is monitored by the Facilities & Infrastructure Manager monthly as the manager reviews all access logs, including badge swipe logs, visitors' logs, and contractor activities. This is also reviewed by the Executive Director of ITS Enterprise Infrastructure Services (EIS) and the IT Security Office Director, as indicated in the Requirements Section.
- Meetings are performed daily to include passing down information upon the arrival of the manager, and daily logs (Generated by the FIOPS staff) are reviewed as well.
- The FIOPS Manager performs a walkthrough of the data center twice weekly to ensure that there are no outstanding issues.

EXCEPTIONS:

None

DEFINITIONS AND ACRONYMS:

Terminology or Acronym	Definition
Colocation Customer	A university faculty or student who has been approved and given access to the data center to maintain and manage their computer systems.
Genie Lift	A material lift that can be used as a hand truck, forklift, or dolly.
Power Distribution Unit (PDU)	A device fitted with multiple outputs designed to distribute electric power, especially to racks of computers and networking equipment located within a data center.
Uninterruptible Power System (UPS)	An electrical apparatus that provides emergency power to a load when the input power source or main power fails.

REVIEW SCHEDULE:

Annually

APPROVAL:

Title, Department Name	Name	Signature and Date
Manager, ITS Enterprise Infrastructure Services – Facilities & Infrastructure Operations	Jerry Ray Peters	Signed by: Jerry Peters 4B7596C7CAA9475... 9/29/2025
Executive Director, ITS Enterprise Infrastructure Services	Ben Allen	Signed by: Ben Allen 02AB20D3D861498... 9/30/2025

REVISION HISTORY:

Date	Version Number	Department or Author	Brief Description of Changes
3/15/2019	1.0	ITS EIS Facilities & Infrastructure Operations	Initial release
3/30/2020	1.1	ITS EIS Facilities & Infrastructure Operations	Reviewed with minor changes – corrected policy name for University Policy #1311 and reformatted standard using updated template
12/10/2020	1.2	ITS EIS Facilities & Infrastructure Operations	Minor updates – clarified and added additional standards
10/12/2022	1.3	ITS EIS Facilities & Infrastructure Operations	Document reformatting and revising NIST 800-53's version number
9/12/2023	1.4	ITS EIS Facilities & Infrastructure Operations	Annual review with minor edits

Titles and department names are subject to organizational changes.

10/14/2024	1.5	ITS EIS Facilities & Infrastructure Operations	Annual review with minor edits – updated document using the new George Mason University logo, colors, and editorial specifications.
9/26/2025	1.6	ITS EIS Facilities & Infrastructure Operations	Annual review with minor edits

RELATED DOCUMENTS/REFERENCES:

- Library of Virginia, General Schedule No. GS-108, Fire, Safety, and Security (Dec 2013)
- NIST Special Publication 800–53 (Revision 5), Recommended Security Controls for Federal Information Systems and Organizations, Moderate Impact Control, Tailored
- University Policy Number 1114, Data Stewardship
- University Policy Number 1305, Reporting Electronic Security Incidents
- University Policy Number 1311, Information Technology Security Program
- University Policy Number 2202, Flexible Work
- Data Center Access Process (ITS.EIS-PRS004)

Titles and department names are subject to organizational changes.