OKLAHOMA
Office of Management
& Enterprise Services

Lincoln Data Center and Whitespace Standard

Introduction

This standard applies to all personnel, customers, contractors and vendors who access, operate, maintain or support the Data Center, DMARC and Industrial Control Systems (ICS) Operational Technology (OT) owned and managed by the State of Oklahoma. It establishes the minimum requirements for physical security, safety, equipment installation, environmental controls and operational procedures to ensure the confidentiality, integrity and availability of data center resources and to maintain a safe working environment.

Purpose

The purpose of this standard is to establish clear and consistent direction for the secure, safe and efficient operation of the State of Oklahoma's data center. This document defines the physical access requirements, safety protocols, equipment handling rules and infrastructure standards necessary to protect critical IT assets, maintain service availability and ensure compliance with state policies. It applies to all personnel, vendors and visitors who access or perform work within these controlled environments.

Definitions

Access control system – an electronic system that restricts and logs physical entry to the Data Center, including badge readers, biometric scanners and security cameras.

Authorized personnel – individuals who have been granted permission to access the Data Center based on affiliation, role and completion of required security clearance.

Cold aisle – the aisle in a data center where cool air is supplied to the front of server racks to maintain optimal operating temperatures.

Data Center customer – any individual or organization affiliated with the State of Oklahoma that uses the Data Center services or space for hosting IT equipment.

Data Center management – Data Center management refers to the designated leadership defined in the escalation section of this document.

Data Center team – the Data Center team is the designated group within OMES Infrastructure responsible for the day-to-day operational oversight, safety and standards enforcement within all defined Data Center spaces, including whitespace, DMARC rooms, staging areas and any VESDA-protected zones.

DMARC (demarcation) room – a physical network room where a service provider's network connects to a customer's network (a demarcation point).

Emergency Power Off (EPO) – a safety feature that allows immediate shutdown of electrical power in the event of an emergency to protect personnel and equipment.

Hot aisle – the aisle in a data center where hot air is expelled from the back of the server racks, away from cooling supply.

Rack unit (U) – a unit of measurement for the height of equipment mounted in a rock, where 1U equals 1.75 inches (44.45 mm).

Thirty-party vendor – An external company or individual contracted to provide maintenance, support or other services within the Data Center.

Tailgating – unauthorized entry into a secure area by following closely behind an authorized person without proper authentication.

Unpacking/Staging Area – designated space outside the Data Center where equipment and materials are unpacked and prepared before instillation.

Very early smoke detection system (VESDA) – an advanced, proactive smoke detection system designed to detect fire at the earliest stages.

Standard

Responsibilities

	Capital Assets Management (CAM)	OMES Infrastructure / Operations	OMES Disaster Recovery / Business Continuity	OMES Cyber Security
Maintain access control systems	C	C	I	R/A
Approve/deny data center access	C	I	I	R/A
Monitor access logs	I	C	I	R/A
Data center key/lock security	I	C	I	R/A
Manage physical assets, inventory and lifecycle	C	R/A	C	C
Equipment installation/deployment/decommissioning coordination	C	R/A	I	C
Environmental & safety	R/A	C	I	C
Enforce data center standards & procedures	C	R/A	C	C
Vendor escorting & oversight	C	R/A	I	C
Incident escalation & operational response	C	R/A	I	C
DR/BC planning & maintaining reliance requirements	C	C	R/A	C
Participation in DR exercises	C	C	R/A	C
Recovery coordination during events	C	C	R/A	C
Communication & Change Management	C	R/A	I	C
DR/BC-related customer communications	I	C	R/A	C
Identify and document potential risks	R/A	R/A	R/A	R/A

Key:

R = Responsible (executes the work)
A = Accountable (final owner of the outcome)
C = Consulted (provides input)
I = Informed (kept notified)

Escalation

Role	Contact	Contact Number	Email
Senior Director of Infrastructure	Jason Nichols	405-522-5702	jason.nichols@omes.ok.gov
Chief Technology Officer of Infrastructure and Operations	David Martin	405-522-6830	david.martin@omes.ok.gov
Chief Information Officer	Dan Cronin	NA	dan.cronin@omes.ok.gov

*For non-emergency items requiring CAM engagement, a Limble ticket may be submitted.
**Full details on submitting Limble tickets may be found in ServiceNow .

1. Defined boundaries.
For the purposes of this standard, the Data Center encompasses all physical spaces, controlled environments and operational areas required to support the secure, reliable and compliant operation of State of Oklahoma data center infrastructure. These boundaries establish where Data Center rules, access controls, safety protocols, equipment-handling requirements and Data Center team oversight apply.

1.1 Whitespace.
Whitespace refers to the primary operational floor containing:

- Server cabinets and racks.
- Power and network distribution equipment.
- Cooling pathways, airflow-dependent layouts and environmental controls.

Whitespace is considered the core of the Data Center and is subject to the highest level of physical security and environmental monitoring and operational governance. All equipment installation, maintenance and technical work must comply with the standards established in this document.

1.2 DMARC rooms.
DMARC rooms are included within Data Center boundaries due to their roles as critical network ingress and egress points. These spaces:

- Serve as the interface between carrier networks and state infrastructure.
- Require strict adherence to access controls, vendor escorting and equipment-handling rules.
- Are governed by the same physical security and environmental requirements as whitespace.

1.3 Staging Areas.
Any spaces protected by a VESDA (Very Early Smoke Detection Apparatus) system is included within the defined Data Center boundary. These areas require:

- Strict environmental controls.
- Restriction of dust- or particulate-generating activities.
- Additional safety and work-practice limitations.

2. Physical access.
Requests for physical access shall be submitted via ServiceNow Catalog Item to the Physical Security team for review/processing.

- All personnel requiring data center access shall complete required training and sign a formal acknowledgement prior to access being granted; acknowledgement shall be retained on file and renewed annually.
- Procedures for obtaining data center access, including after-hours and emergency access, shall be documented, communicated to all authorized personnel and referenced within the access request process.
- All Data Center personnel must present and carry valid State of Oklahoma identification at all times while working in the Data Center, whether as a physical security badge or a kiosk-issued IS badge.
- Authorization applies only to the named individual; access is non-transferrable and does not permit that individual to extend access to others.
- Thirty-party vendors providing IT support shall only enter the facility when escorted by an authorized Data Center staff member.
- Thirty-party vendors shall always be escorted by an authorized Data Center team member while in the Data Center. Any tours of the facility must be coordinated directly with State of Oklahoma executive staff.
- Data Center doors must remain locked or secured at all times. Doors are never to be held, wedged, blocked, braced, jammed, forced, left over or kept ajar.
- Extreme caution must be exercised to prevent unauthorized persons from gaining access through "tailgating".
- All personnel shall be trained on tailgating prevention, the non-transferable nature of access authorization and third-party escort requirements; unauthorized access attempts or policy violations must be reported immediately to the Data Center manager or designee.
- All physical access must be logged via the access control system; logs are retained for a minimum of one year.
- Video surveillance is active in all sensitive areas.
- Violations of physical access policies shall be subject to a formal accountability process; repeated or egregious violations may result in access revocation and escalation to agency leadership.
- Photography is strictly prohibited without formal approval and release from Data Center management.

3. General Work Rules.

- Use of tobacco and/or vape products is prohibited within all State of Oklahoma buildings.
- Food and drink, including sealed containers, are prohibited within the Data Center.
- Liquids of any kind are not permitted inside the Data Center.
- All unpacking activities must occur outside the Data Center in designated staging areas; no cardboard, plastic, packing peanuts, paper wrap, wood or similar materials are allowed inside.
- The Data Center team must be consulted before installing any new equipment to confirm adequate space, power and cooling availability.
    - Electrical modifications shall be coordinated with CAM and shall be completed by a CAM approved electrician. End rack PDU documentation shall be updated with any electrical changes.
- Leaning against any walls or equipment, and placing or hanging clothing, tools, test devices, or any other items on equipment, is strictly prohibited.
- Auxiliary air-handling or air-movement devices – including fans, shop vacuums, floor vacuums or any other non-permanently installed equipment – are not permitted within the Data Center. The use of such devices may trigger sensitive equipment environmental

controls, including the FM-200 fire suppression system, due to the risk of releasing airborne particles.

- Every effort shall be made to minimize airborne dust or particulates of any type within the Data Center.
- Work requiring open flame is strictly prohibited within the Data Center whitespace.
- Data Center management reserves the right to exclude or remove individuals from the facility; requests to leave must be followed promptly and peacefully.
- Customers and visitors are responsible for their personal belongings while on the premises.
- Failure to comply with the requirements outlined in this standard will result in immediate removal from the data center whitespace and the revocation of future access rights. Third-party vendors who fail to comply will face the same removal and loss of access, along with a formal supplier complaint for non-compliance.

4. Safety

- Removal of equipment in extreme cases (e.g., equipment that poses a fire hazard or a cybersecurity risk), the Data Center management reserves the right to physically disconnect and/or remove the hardware.
- No network cables or power cords may be strung along the floor to prevent tip hazards.
- Due to high noise levels, hearing protection is recommended; personal audio devices (earphones, headphones) for music are discouraged and do not substitute hearing protection.
- Closed-toe footwear must be worn inside the Data Center.
- Safety cones, barricades, caution tape and other safety equipment must not be moved or bypassed.
- The Data Center and staging areas must be kept clear and free of debris. All personnel are expected to clean up after activities.

5. Server Cabinet Systems.

5.1 Cabinet standards.

- Authorization from Data Center management must be obtained prior to the purchase or acquisition of any new racks or enclosures. This ensures compatibility with existing infrastructure, power and cooling standards.
- Racks must have 42U vendor-neutral mounting rails, adjustable and compatible with all EIA-310 compliant 19” equipment.
- Cabinets must have access points for power and data pathways at both the top and bottom.
- The Data Center will maintain a standardized set of cabinets tailored to site-specific needs.
- Cooling shall be achieved by traditional air-based means. Liquid (immersion and/or Direct to Chip) cooling is prohibited.
- Keys for any server racks, cabinets or enclosures shall never be left inserted in, hanging from or stored on any rack or cabinet within the Data Center whitespace, SMARC rooms or any VESDA-protected area.
- All racks and enclosures must always remain locked, unless an authorized individual is actively working inside the enclosure.

5.2 Cabinet layout.

- Cabinets will be arranged in a hot/cold aisle configuration.
- Cold aisle edges of equipment enclosures must align with floor tile edges.

- Aisles must be wide enough to ensure equipment access and a safe workspace.
- Where vented floor tiles are insufficient, additional cooling measures will be implemented.
- Blanking panels must be installed in unused rack space to minimize hot/cold air mixing.

5.3 Cabinet loading.

- Rack weight per contact point (caster or leveling foot) shall not exceed the installed panel's concentrated load rating.
    - Installed raised floor system: Tate ConCore CCN1250/bolted stringer – 1,250 lb. concentrated, 6,000 lb. pedestal axial, 1,000 lb. rolling (10 passes), per CISCA A/F.
- Cumulative load at any shared pedestal shall not exceed the pedestal's axial load rating.
- Rack relocation across the raised floor shall not exceed the panel's published rolling load rating.
- Rack heat load must not exceed the cooling capacity of the area.
- Common densities per the Uptime Institute advise 4kW to 6 kW per rack.
- Large or heavy equipment must be installed at the bottom of racks.

5.4 Cabinet power.

- No internal power connections are allowed between adjacent racks or cabinets.
- Power strips must have dedicated home runs back to their power source.
- Power strips must not be daisy-chained and must be securely mounted within the rack.
- Cable management must be maintained to avoid airflow obstruction.
- Non-IT listed devices, including but not limited to, USB-powered, PDU-powered, battery-operated or independently circuited lighting fixtures, shall not be installed, mounted, affixed or otherwise placed within any server rack, cabinet or enclosure on the data center whitespace floor. All lighting requirements shall be addressed exclusively through facility-level overhead lighting systems.

6. *Raised flooring*.

6.1 Structural safety limits.

- Adjacent tiles: do not remove more than two (2) adjacent tiles at any time. Removing more than two tiles in a cluster removes the lateral support for the surrounding pedestals, significantly increasing the risk of a "domino effect" collapse if bumped.
- Linear removal: never remove more than five (5) tiles in a single line. If a trench is required, use temporary "stringers" or bridge supports to maintain the grid's rigidity.
- Buffer zones: Always maintain a minimum of four (4) secure tiles in every direction between open areas. This "checkboard" approach ensures the lateral load is distributed across the remaining grid.

6.2 Environmental & airflow control.

- Static pressure: to prevent a drop in sub-floor static pressure, keep tiles closed whenever work is not being actively performed.

- Bypass air: every open tile acts as a “chimney”, stealing cold air from the equipment racks. If more than 2% of the total area is open, cooling efficiency drops by as much as 30-50% in high-density zones.

6.3 Hazard mitigation.

- Barricades: any floor opening left unattended for more than 1 minute must be surrounded by a physical safety barrier or guarded by a “spotter”.
- Tile handling: tiles should be stacked no more than 5 high to prevent overloading the local grid and should be placed “face-to-face” to protect the HPL (High-Pressure Laminate) surface.

7. Environmental monitoring and fire safety.

- Environmental sensors (temperature, humidity, smoke) must be installed and monitored continuously.
- Fire suppression systems are required and regularly maintained.
- Emergency exits and fire alarm procedures must be clearly posted.
- Fire extinguishers must be easily accessible and inspected regularly.

8. Emergency procedures.

- Emergency Power Off (EPO) buttons must be clearly labeled and protected against accidental use.
- All data center personnel shall complete initial training during onboarding and recurring training no less than annually, with additional refresher conducted as needed; training curriculum shall include emergency evacuation procedures, FM-200 suppression system protocols, the Data Center Physical Security Standard and third-party escort policies and expectations. Procedures for power failures, fires and other emergencies must be defined and communicated.

9. Maintenance and change management.

- All physical changes (equipment installation, removal or moves) require prior documentation and approval through the established Change Management Process.
- Maintenance activities must be scheduled and documented to minimize service disruption.
- Access lists must be reviewed quarterly; terminated personnel must have access revoked within 24 hours.

10. Cabling standards.

- Network and power cables must be color-coded and labeled on both ends.
- Patch panels are required for structured cabling; direct cabling to switches should be avoided.
- Cable bundling should use Velcro ties instead of zip ties to prevent damage.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To ensure efficient, secure, and cost-effective delivery of essential public services, all state agency IT purchases and projects must receive central approval. This allows the Chief Information Officer to evaluate agency needs and capabilities, strengthen data protection and security, and streamline and consolidate systems to reduce costs for taxpayers.

References

- LIMBLE ticket for CAM engagement.
- Information on LIMBLE tickets for the Lincoln Data Center.
- Physical access request form.
- Physical Security Standard.
- Change Management Standard.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 06/02/2026	**Review cycle:** Annual
Last revised: 06/01/2026	**Last reviewed:** 06/01/2026
Approved by: Dan Cronin, Chief Information Officer	