

2.8 Technology Resource Physical and Environmental Security Standard

Effective Date: July 1, 2026

Revised Date: July 1, 2026

1. Purpose

This standard establishes the mandatory requirements for assessing, managing, and monitoring the physical and environmental risk associated with technology resource management and card access management for Arkansas State University. The purpose of this standard is to ensure that these risks are managed in a consistent manner that protects university data and mitigates institutional risk.

2. Scope

This standard applies to all data, personnel, assets, information management systems, and technology resources under the responsibility of Information and Technology Services (ITS). Where applicable, some physical and environmental security controls will not be covered in this standard as their responsibility lies outside of Information and Technology Services.

3. Definitions

Technology Resources – The machines, devices, systems, services, and related components used in information processing. This includes:

- Machines, devices, and transmission facilities used in information processing, such as computers, word processors, terminals, telephones, cables, software, and related products.
- Devices used to process information through electronic capture, collection, storage, manipulation, transmission, retrieval, and presentation of information in the form of data, text, voice, or image, including telecommunications and office-automation functions.
- Any component related to information processing and wired or wireless telecommunications, including hardware, software, services, planning, personnel, facilities, and training.
- Procedures, equipment, and software designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, along with associated personnel such as consultants and contractors.
- All email accounts issued by the Arkansas State University System.

Credential-Based Electronic Physical Access - The use of electronic access control systems that authenticate an individual's identity through a unique, assigned credential before permitting physical entry to a secured area. Credentials may include card-based, mobile, biometric, PIN-based, or other industry-standard authentication mechanisms and are managed, logged, and revoked through centrally administered access control systems.

Intermediate Distribution Frame (IDF) - A secured space that houses building or floor-level network and telecommunications infrastructure, such as switches, patch panels, cable terminations, and related power/UPS equipment, used to distribute connectivity to end-user areas.

Main Distribution Frame (MDF) - The primary building distribution point for network and telecommunications cabling and services; typically the central equipment room where external service-provider circuits enter and where core routing/switching, patch panels, and backbone cabling connect to one or more IDFs.

Data Center - The secured, purpose-built room that houses centralized computing and storage infrastructure, such as servers, virtualization platforms, storage systems, core networking, and supporting management systems, and provides the environmental controls needed to operate them reliably, such as power distribution/UPS, cooling, fire detection/suppression, and monitoring, for Arkansas State University.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of applicable state and federal compliance frameworks. This includes:

Chief Information Officer (CIO) - Responsible for the executive sponsorship, governance, and oversight of the University's technology resource physical and environmental security processes. Ensures that applicable regulatory, statutory, and contractual obligations are identified, translated into actionable controls, and operationalized across institutional systems and processes.

Card Center - Responsible for ordering, configuring, maintaining, and coordinating the effective management of physical and environmental security relating to credential-based electronic controls. This includes IDF, MDF, and Data Center security controls utilizing credential-based electronic access controls.

Telecomm Services - Responsible for configuring, maintaining, and coordinating the effective management of physical and environmental security relating to infrastructure such as cabling, hardware installation, and infrastructure repairs or replacements. Responsible for the auditing of all IDF and MDF locations to ensure spaces are not improperly utilized.

ITS Networking Team - Responsible for configuring, maintaining, and coordinating the effective management of environmental monitoring controls within university MDFs.

Access Approval Board (AAB) - Responsible for the review and approval of Tier 2 access requests.

University Police Department (UPD) - Responsible for initiating and coordinating university-wide credential-based electronic physical access events such as campus-wide lockdowns or shelter-in-place orders.

5. Standard Exceptions

The Chief Information Officer for the Campus is authorized to review and approve exceptions to this standard when organizational needs justify a deviation, and the associated risks are deemed acceptable. All exceptions must be documented, including a defined scope, a scheduled review date, and compensating controls when appropriate. The CIO may delegate this authority as necessary but retains overall accountability for exception management and review.

6. Credential-Based Electronic Physical Access Security Controls

Arkansas State University primarily utilizes University ID cards as the primary credential-based electronic physical access mechanism to campus facilities and university services. These ID cards are managed to the following minimum standards:

- Identity verification using a government-issued ID is required prior to issuing university ID credentials to ensure that credentials are only assigned to verified individuals.
- University ID credentials must be logged and maintained within the university's credential management system.
- University ID credentials may also support additional services including identification, campus transactions, and other institutional functions.

Temporary credential-based electronic physical access mechanisms may be issued to contractors, vendors, project personnel, or other members of the campus community as deemed necessary. These credentials must:

- Be approved by designated building or departmental contacts.
- Be assigned only for the duration of the authorized period.
- Be tracked through documented checkout procedures.
- Be returned upon the end of the authorized period.

All credential holders are responsible for safeguarding university-issued credentials and preventing unauthorized use. Lost or stolen credentials must be reported to the Arkansas State University Card Center immediately so that compromised credentials can be disabled within the access control system.

7. Credential-Based Electronic Physical Access Request Tiers

Access Request Tier	Requirements
Tier 1	• Internal to internal requests, including approved A-State vendors. • Building contacts required to approve requests.

Access Request Tier	Requirements
Tier 2	• External to internal requests, such as unapproved A-State vendors. • Access Approval Board required to review and approve requests. • Building contacts required to approve requests. • Required for access to be granted to any restricted access location.

8. Credential-Based Electronic Physical Access Requests (Tier 1)

The Arkansas State University Card Center manages and processes requests for access to university facilities that utilize credential-based electronic physical access mechanisms. Requests for access may be submitted by:

- The individual requesting access.
- Supervisors or departmental representatives.
- Authorized building or departmental contacts.

All requests for access must also be reviewed and approved by the designated building or departmental contact responsible for the requested location. Access assignments must reflect operational need and may include restrictions based on:

- Building or facility.
- Interior areas within a building.
- Access schedules.
- Specific operational requirements.

9. Credential-Based Electronic Physical Access Requests (Tier 2)

To ensure the secure and efficient management of physical access requests, Arkansas State University maintains an Access Approval Board (AAB) to review and process access requests. This AAB consists of stakeholders from the University Police Department (UPD), Campus Card Center, and Facilities Management (FM) to vet both credential-based electronic access and key-based access requests.

This AAB allows the critical task of ensuring secure physical access is only granted to those with justifiable need and reduces the risk of irrelevant stakeholders being tasked with granting sensitive access to university facilities. At times, this AAB may reach out to alternate stakeholders depending on the scope and timing of the access.

10. Credential-Based Electronic Physical Access Auditing

The Arkansas State University Card Center actively manages and provides oversight to the lifecycle of credential-based electronic physical access mechanisms. This management includes the disablement and auditing of granted access in alignment with the following requirements:

Account Status Monitoring

- Account status information is maintained through institutional systems and automated processes.
- Credential systems may receive updates through university data sources used to determine account eligibility.
- Access privileges must reflect an individual's current affiliation with the university.

Access Removal

- Access credentials must be removed when individuals are no longer authorized to access university facilities.
- Situations requiring access removal include, but are not limited to:
 - Employee termination.
 - Student status changes.
 - Expiration of temporary credentials.
 - Loss of authorization from departmental contacts.
- Once an account is deactivated, associated credentials including physical cards, mobile credentials, and biometric credentials will cease functioning within the access control system.

Automated Credential Management

- Automated processes may be used to review account status and disable credentials associated with inactive accounts.
- These processes support consistent access lifecycle management and help prevent unauthorized access when individuals are no longer affiliated with the university.

Door Position Sensor Review

- Credential-based electronic physical access doors are actively monitored for their position to ensure they are not propped open, damaged mechanically, or tampered with leading to the sensor identifying the door as not secured.
- Identified doors are reviewed and escalated if not resolved within a procedurally defined timeframe.
- Building contacts receive automated reports of all authorized individuals with credential-based electronic physical access to their responsible building(s) or area(s). This report is then reviewed and access updated in accordance with the building contact's feedback.

11. Continuity of Technology Resource Operations

Arkansas State University ITS shall maintain a supplemental Business Continuity & Disaster Recovery Plan, separate from this standard, that outlines how the IT organization plans to ensure continuity of business operations and recovery from an environmental disaster. This includes requirements and controls surrounding the continued operation of infrastructure necessary to the physical and environmental security requirements within the scope of this standard.

12. Physical Infrastructure Installation Requirements

The Arkansas State University Telecomm Services and Networking Team shall maintain supplemental procedure(s), separate from this standard, that outline how physical infrastructure is installed and maintained in accordance with state, federal, and university regulations and policies. At a minimum, this will include and establish the following subjects:

- Contractor and sub-contractor minimum requirements that must be met for a potential contract to be awarded.
- Network cabling requirements such as rating, plenum vs. non-plenum, shielding, and coloring.
- Every network cable installed will be labeled at the jack and on the patch panel. No label will be handwritten.
- Exposed wiring requirements.
- Ladder rack, closet rack, patch panel, and outlet cover requirements.
- Fiber optic cabling and connector requirements.
- Conduit and cabling, copper and fiber, installation procedures.
- MDF and IDF minimum requirements.
- Emergency infrastructure installation requirements.
- Fireproofing and code enforcement requirements for installations or building modifications resulting from physical infrastructure installations.

13. MDF and IDF Physical Access Security Controls

To ensure the secure operations of critical technology resource infrastructure across Arkansas State University, MDF and IDF locations are required to be secure, purpose-focused, and access restricted. The following requirements outline the minimum and recommended requirements for access controls to these spaces.

Minimum Requirements

- The room cannot be a shared space or utilized for any unauthorized purpose, such as custodial closet, general storage, or general workspace.
- The room must have points of entry that can be restricted to the general public.
- Point(s) of entry must be secured with key-based access control.
- Key-based access control must be limited to ITS personnel only.
- Keys shall be managed only by ITS personnel.

Recommended Requirements

- Key-based access control must be limited to ITS personnel only.
- Keys shall be managed only by ITS personnel.
- The room cannot be a shared space or utilized for any unauthorized purpose, such as custodial closet, general storage, or general workspace.
- The room must have points of entry that can be restricted to the general public.
- Point(s) of entry must be secured with credential-based electronic access control.
- Secondary or alternate key-based access control must be limited to ITS personnel only.

- Secondary or alternate key-based access control must be utilized only if primary credential-based electronic access control is unavailable.
- Keys for the alternate access method must be stored within the university Data Center and strictly managed and controlled.
- All point(s) of entry must have security camera coverage ensuring entry and exit from the space is recorded.

14. MDF and IDF Environmental Security Controls

To ensure the secure operations of critical technology resource infrastructure across Arkansas State University, MDF and IDF locations are required to be monitored for environmental factors that could impact the operations of the infrastructure. The following requirements outline the minimum and recommended requirements for environmental controls in these spaces.

Minimum Requirements

- The room must contain fire detection and fire suppression systems.
- The room must have UPS and surge protection equipment installed in alignment with Business Continuity and Disaster Recovery plan specifications.
- The room must be temperature controlled via HVAC.

Recommended Requirements

- The room must contain fire detection and fire suppression systems.
- The room must have UPS and surge protection equipment installed in alignment with Business Continuity and Disaster Recovery plan specifications.
- The room must be temperature controlled via HVAC.
- The room must be equipped with temperature monitoring sensors that alert ITS staff if temperatures fall outside acceptable thresholds.
- The room must be equipped with humidity monitoring sensors that alert ITS staff if the humidity falls outside acceptable thresholds.
- The room must be equipped with water detection sensors that alert ITS staff if water is detected within the room where it could impact the operation of equipment.
- HVAC control of the room is located only within that room and is not dependent on the temperature of another room.

15. MDF and IDF Physical and Environmental Security Auditing

To ensure the secure operations of critical technology resource infrastructure across Arkansas State University, MDF and IDF locations are required to be audited on a regular basis for factors that could impact the operations of the infrastructure. The following requirements outline the minimum and recommended requirements for auditing these spaces.

Minimum Requirements

- Weekly: ensure room cleanliness, verify airflow is unobstructed, confirm power status, and check for unauthorized access.

- Quarterly: conduct a cable management inspection, update network topology, check panel connections, ensure all cables are labeled, and remove any unused equipment.
- Annually: assess cable capacity, review security procedures, and complete a full inventory of all equipment.

Recommended Requirements

- Conduct weekly checks to ensure that room temperature and humidity levels remain within the designated acceptable range.
- Conduct a comprehensive review of the infrastructure on an annual basis and identify any necessary upgrades or enhancements.

16. Restricted Access Location Establishment & Management

Certain university facilities and locations require enhanced access controls due to the sensitivity of operations, equipment, or information physically secured at the facility. These facilities, designated as restricted access locations, must remain secured and accessible only through authorized credentials and are beholden to the following requirements:

- Public access to these facilities is not permitted without authorization or escort.
- Access permissions must be limited to individuals whose job responsibilities require entry.
- Access may be restricted by location, area within the building, or defined access schedules.

Within restricted facilities, internal areas may be secured through additional access control mechanisms. These controls may include:

- Continuous locked access.
- Scheduled door access.
- Restricted access to designated personnel.

To ensure the ongoing integrity, safety, and operational reliability of restricted access locations, including but not limited to IT closets, IDFs, MDFs, and similar infrastructure spaces, the following establishment, management, and audit requirements must be met:

Minimum Requirements

- Restricted access locations must be purpose-built or designated solely for technology infrastructure and must not be used for general storage, custodial purposes, or unrelated activities.
- The space must be free of debris, combustible materials, and any items that may obstruct access, airflow, or safe operation of equipment.
- The room must have adequate power distribution and surge protection to support installed equipment.
- The room must be supported by HVAC systems sufficient to maintain safe operating temperatures for installed technology.

- The room must have fire detection and suppression systems in place in accordance with applicable fire and safety codes.
- The room must be included in a formally documented audit process managed by ITS.
- Audits must be conducted at least annually to validate compliance with physical and environmental requirements.
- Identified deficiencies must be documented and remediated within a defined and tracked timeframe.

Recommended Requirements

- The room should be equipped with Uninterruptible Power Supply (UPS) systems to provide temporary power continuity and protection from power fluctuations.
- The room should include temperature monitoring sensors capable of alerting ITS personnel when thresholds are exceeded.
- The room should include humidity monitoring sensors capable of alerting ITS personnel when thresholds fall outside acceptable ranges.
- The room should include water detection sensors positioned to identify leaks or moisture intrusion that could impact equipment.
- Environmental monitoring systems should be centrally managed and integrated with alerting/notification platforms.
- A standardized audit checklist should be maintained and used to ensure consistency across all restricted access locations.
- Audit results should be retained for reporting, compliance validation, and continuous improvement efforts.
- Locations failing to meet minimum standards should be escalated to appropriate leadership and prioritized for remediation based on risk level.

17. Restricted Access Location – University Data Center

The university data center maintains a restricted access location status and is secured at all times. Entry is restricted to authorized individuals who must authenticate through the university's access control system, with multi-factor authentication applied where available. In emergency situations, physical key access may be provided to authorized staff under strictly controlled protocols.

Access to the university data center cannot be authorized for users who have not completed Criminal Justice Information Services (CJIS) training.

18. Restricted Access Location – Library Backup Data Center

The backup university data center, located in the Dean B. Ellis Library, maintains a restricted access location status and is secured at all times. Entry is restricted to authorized individuals who must authenticate through the university's access control system, with multi-factor authentication applied where available. In emergency situations, physical key access may be provided to authorized staff under strictly controlled protocols.

Access to the backup university data center cannot be authorized for users who have not completed Criminal Justice Information Services (CJIS) training.

19. Restricted Access Location – Admin Annex Primary Telecomm Demarc

The primary telecommunications demarc, located in the Administration Annex Building, maintains a restricted access location status and is secured at all times. Entry is restricted to authorized individuals who must authenticate through the university's access control system, with multi-factor authentication applied where available. In emergency situations, physical key access may be provided to authorized staff under strictly controlled protocols maintained by responsible parties outside of ITS.

20. Campus Partnerships

Arkansas State University ITS partners with various stakeholders across the Jonesboro campus to ensure the physical and environmental security of both the technology resources in use and of the students, faculty, and staff. These partnerships include:

- University Police Department (UPD)
- Facilities Management, including physical key management
- Building stakeholders, including access approval

21. Vendor Management

Physical access to university facilities and locations, including restricted access locations, by vendors must follow the University's Data Center Access Procedure as well as prior approval from the Vendor/Contractor Access Request Form. Vendors may be required to sign a Confidential Information Agreement before accessing A-State systems. All access granted is temporary and purpose specific.

External vendors must comply with all relevant university policies, standards, and procedures while granted access beyond that of the public. Failure to comply with these may result in removal of access and future restrictions or rejection of access requests.

22. Standards Review

This document will be reviewed and reaffirmed annually, or upon significant changes to university IT governance, systems, or regulatory requirements.

Effective Date: July 1, 2026

Next Review Date: July 1, 2027

Version: 1.0

Referenced Policies, Standards, and Procedures

- Business Continuity and Disaster Recovery Standard

Revision #1

Created 2026-06-26 02:15:30 UTC by Christopher Boothman

Updated 2026-06-26 02:18:48 UTC by Christopher Boothman