Standards

Browse approved IT standards that define technical requirements, security expectations, and implementation guidelines across the organization. These resources help ensure consistency, accountability, and alignment with regulatory and industry best practices

- 2.1 Artificial Intelligence Governance Standard
- 2.2 Business Continuity and Disaster Recovery Standard
- 2.3 Compliance Framework Implementation and Assurance Standard
- 2.4 Enterprise Resource Planning (ERP) Standard
- 2.5 Network Security Standard
- 2.6 Risk Assessment and Vendor Management Standard
- 2.7 Technology Resource Management Standard
- 2.8 Technology Resource Physical and Environmental Security Standard
- 2.9 Technology Resource User Education Standard
- 2.10 Vulnerability and Patch Management Standard
- 2.11 Logical Access Security Standard
- 2.12 Records Retention Standard
- 2.13 Institutional Asset and Device Naming Standard
- 2.14 Mobile Hotspot and MiFi Usage Standard
- 2.15 Electronic Forms Creation & E-Signature Standard

2.1 Artificial Intelligence Governance Standard

> **Applicability Statement**
> This standard governs the use, procurement, development, administration, and oversight of Artificial Intelligence (AI) and Automated Decision Tools (ADT) when used on Arkansas State University-owned or managed technology resources, or when used to conduct official university business, regardless of whether those activities occur on university-owned or personally owned devices.
>
> This standard is not intended to govern the academic use of AI by students for coursework, assignments, research, or other learning activities, except when students are acting on behalf of the university in an employment or official institutional capacity. Students should refer to the Arkansas State University Ethical Use of Artificial Intelligence Policy, applicable academic integrity policies, and any college-, department-, or course-specific AI requirements established by their instructors regarding permissible uses of AI in academic work.

Effective Date: July 1, 2026
Revised Date: July 1, 2026

1. Purpose

The purpose of this standard is to establish the required controls, governance, and operational requirements for the use of Artificial Intelligence (AI) and Automated Decision Tools (ADT) within the Arkansas State University (A-State) environment. This standard ensures that AI technologies are used ethically and in compliance with applicable laws, regulations, and university policies.

2. Scope

This standard applies to all faculty, staff, students, contractors, affiliates, and members of the A-State community who use, develop, or oversee Artificial Intelligence or Automated Decision Tools when conducting university business or using university technology resources. This standard applies to all institutional data as governed by the Data Security and Classification Policy and applies in all work settings, including on campus, remote work locations, and approved telecommuting arrangements.

3. Definitions

Artificial intelligence - A machine-based system that can, based on a given set of human-defined objectives, make predictions, recommendations, or decisions influencing a real or virtual

environment.

Automated decision tool - A system or service that uses artificial intelligence and has been specifically developed and marketed, or specifically modified, to make or to be a controlling factor in making consequential decisions.

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.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates, and members of the system community.

System Community - Any person who accesses the ASU System's IT infrastructure who is not classified as a member of the faculty, staff, or enrolled student.

Systems Authority - ASU System delegates oversight of particular systems to the head of a specific unit of the ASU System or to an individual faculty member, in the case of technology resources purchased with research or other funds for which he or she is personally responsible.

Systems Administrator - A Systems Authority may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular technology resources.

Certifying Authority - This is the Systems Administrator or other ASU System authority who certifies the appropriateness of an official ASU System document for electronic publication in the course of ASU System business.

Specific Authorization - This means documented permission provided by the applicable Systems Administrator.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of controls necessary to ensure the effective management and remediation of technology resource vulnerabilities. This includes:

Chief Information Officer (CIO) - Responsible for the executive sponsorship, governance, and oversight of the University's artificial intelligence governance processes within the scope of this standard. Ensures that applicable regulatory, statutory, and contractual obligations are identified, translated into actionable controls, and operationalized across institutional systems and processes.

Data Custodians (Digital Records) - Responsible for implementing and operating the technical and administrative controls that protect digital institutional data in accordance with applicable compliance frameworks and institutional policy.

Human Resources – Responsible for the maintenance and enforcement of disciplinary requirements outlined in this standard.

Employee Training & Development Authority – Responsible for the coordination of user training requirements, assignment, and record maintenance outlined in this standard.

Procurement Services - Responsible for developing and maintaining processes for the procurement of Artificial Intelligence, Automated Decision Tools, and any third-party platform in partnership with ITS. Responsible for ensuring that risk assessments are performed prior to procurement.

ITS – Responsible for developing and maintaining processes for the procurement of Artificial Intelligence, Automated Decision Tools, and any third-party platform in partnership with Procurement Services. Responsible for maintaining a centralized inventory of all approved AI and ADT Systems.

IT Security – Responsible for completing adequate security risk assessments within the processes maintained by ITS and Procurement Services.

5. Standard Exceptions

The Chief Information Officer 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.

6. Approved AI Tools and Platforms

A-State users are not authorized to use AI or ADT tools that have not been formally reviewed and approved via ITS and Procurement Services vetting processes. To view live applications that have been approved for institutional use, please access the link below.

Approved Software Directory

7. Artificial Intelligence Assistants

Artificial Intelligence powered meeting transcription and recording tools, such as those integrated into Microsoft Teams or Zoom, are not appropriate for all settings and should only be used in meetings where their presence aligns with meeting objectives, privacy expectations, and institutional policy.

Examples where AI assistants are not permitted include, but are not limited to:

- Any discussion involving regulated data, including FERPA, HIPAA, or CJIS data.
- Any discussion without the informed consent of all attendees and participants.
- Any AI Assistant added to a discussion by a contractor, affiliate, or member of the system community.

All Artificial Intelligence powered meeting transcription and recording tools must be approved through the standard procurement processes as dictated by Procurement Services. This includes any tools that are available for use free of charge.

8. Data Classification

To ensure alignment with the Arkansas State University System Artificial Intelligence Governance Policy and the Data Classification and Security Policy, this standard establishes the following requirements:

- Public data may be used with AI tools as long as no sensitive non-publicly available data is included.
- Internal data is permitted for entry to AI agents, tools, and processing methods on A-State maintained and approved platforms.
- Data classified as confidential or regulated is not permitted for entry to any Artificial Intelligence agent, tool, or processing method unless explicitly authorized.

9. Monitoring and Enforcement

A-State shall monitor university technology resources for unauthorized or inappropriate use of AI or ADT tools. This monitoring includes, but is not limited to:

- Review of network logs to identify unauthorized utilization of AI or ADT tools.
- Review of application installations on university owned and maintained technology resources to identify unauthorized utilization of AI or ADT tools.
- Receipt and subsequent investigation of user reported unauthorized or inappropriate use of AI and ADT tools.

Enforcement mechanisms include, but are not limited to:

- Disablement of the offending user's university account.
- Network containment of noncompliant technology resources.

- Removal of the noncompliant AI or ADT tool from university accounts and technology resources.
- Discipline in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the applicable Handbook.

10. Ethical and Responsible Use of AI and ADT Tools

A-State requires an authorized human user or designee to make any final decision in the course of his or her employment, regardless of what artificial intelligence or automated decision tool the employee or designee recommends.

Use of AI or ADT tools must be ethical, transparent, and aligned with the academic integrity standards and acceptable use standards of A-State. Users remain fully responsible for the accuracy, originality, and compliance of all work produced with AI or ADT assistance.

Users are responsible for disclosing when AI is used for decision making, content generation, or other impactful processes. Unauthorized or undisclosed use of AI or ADT tools may constitute a violation of institutional policy or academic misconduct standards.

11. User Training Requirements

The A-State Employee Training & Development Authority shall develop a training program for all students, faculty, staff, and users of the system concerning the appropriate use of artificial intelligence and automated decision tools in deciding an outcome in the course of their time as an authorized user of the system's technology resources.

This training shall be included and required in all new employee and student training and will be completed on an annual basis.

12. Risk Management Review

Due to the variable risk that comes with AI products and the function they are set to perform, risk levels may be vastly different based on the AI product. In order to properly assess and secure internal or outsourced data, A-State must ensure a risk assessment is performed to identify, assess, and manage risks associated with AI and ADT tools.

This risk assessment applies to standalone AI tools, ADT tools, artificial intelligence powered meeting transcription and recording tools, as well as third-party platforms and integrations that utilize AI to process institutional data.

Security risk assessments will be completed by the IT Security team as part of the Technology and Digital Services Purchase Pre-Authorization review process jointly maintained with Procurement Services and ITS. Security documentation from this review will be annually reviewed and refreshed to ensure security practices are still in alignment with A-State requirements.

Procurement of Artificial Intelligence, Automated Decision Tools, and any third-party platforms and integrations that utilize AI must follow all standard procurement processes as dictated by

Procurement Services.

13. 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

- Artificial Intelligence Governance Policy
- Data Security and Classification Policy
- Faculty, Staff, and Student Handbooks

2.2 Business Continuity and Disaster Recovery Standard

Effective Date: July 1, 2026
Revised Date: July 1, 2026

1. Purpose

This Standard establishes the mechanisms necessary to ensure Arkansas State University (A-State) can maintain or rapidly resume essential academic, administrative, and technology operations following a disruptive incident. This standard aligns institutional service criticality with technical restoration priorities, establishes recovery time objectives (RTO) and recovery point objectives (RPO) expectations, and defines governance, testing, communication, and compliance requirements for ITS.

2. Scope

This standard applies to all Arkansas State University Information Technology Services (ITS)-supported environments, services, and technology resources, including enterprise systems and services such as compute, storage, operating systems, databases, software, and technical documentation; enterprise communications encompassing network infrastructure, VoIP, email, web presence, and ISP or carrier services; ERP application data, including Banner ERP and related systems; and data center facilities, specifically the primary ITS Data Center, as well as cloud-hosted services with verified disaster recovery capabilities.

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.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates, and members of the system community.

System Community - Any person who accesses the ASU System's IT infrastructure who is not classified as a member of the faculty, staff, or enrolled student.

Systems Authority - ASU System delegates oversight of particular systems to the head of a specific unit of the ASU System or to an individual faculty member, in the case of technology resources purchased with research or other funds for which he or she is personally responsible.

Systems Administrator - A Systems Authority may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular technology resources.

Certifying Authority - This is the Systems Administrator or other ASU System authority who certifies the appropriateness of an official ASU System document for electronic publication in the course of ASU System business.

Specific Authorization - This means documented permission provided by the applicable Systems Administrator.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of controls necessary to ensure the effective management and remediation of technology resource vulnerabilities. This includes:

Chief Information Officer (CIO) - Responsible for the executive sponsorship, governance, and oversight of the University's business continuity and disaster recovery processes within the scope of this standard. Ensures that applicable regulatory, statutory, and contractual obligations are identified, translated into actionable controls, and operationalized across institutional systems and processes.

Assistant Vice Chancellor of IT Infrastructure and Operations – Responsible for the planning, execution, and continuous improvement of the University's Business Continuity and Disaster Recovery (BC/DR) program. Oversees all infrastructure-related recovery capabilities, including systems, network, endpoint, and IT support services. Leads incident response and recovery operations for infrastructure services and ensures all ITS teams are aligned with and operating in accordance with this standard.

Assistant Vice Chancellor for ERP Application Services – Accountable for the continuity, recovery, and integrity of the University's Enterprise Resource Planning (ERP) systems and associated data. Leads ERP-specific recovery planning, testing, and execution. Coordinates with the

Assistant Vice Chancellor of IT Infrastructure and Operations during incidents to ensure infrastructure and application recovery efforts are aligned, and ERP services are restored in accordance with defined recovery objectives.

Director of IT Security – Responsible for overseeing the university's IT security program and serves as a member of the Crisis Assessment and Management Team during incident response activities. Works closely alongside the AVC of IT Infrastructure and Operations when incidents are classified as a security incident.

Crisis Assessment and Management Team (CAMT) - Responsible for evaluating incidents, assigning crisis classification, authorizing plan activation, and providing executive updates. This team consists of the CIO as Lead, Director of IT Security, Assistant Vice Chancellor of IT Infrastructure and Operations, Assistant Vice Chancellor for ERP Application Services, and the directors for IT Support, Systems, and Networking.

Crisis Recovery Team (CRT) - Responsible for executing system, application, network, communication, and data restoration activities according to the mapped prioritization and runbooks.

Executive Leadership – Responsible for authorizing major institutional actions, including alternate facilities and public communications. This consists of the Chancellor, CFO/VCFA, Provost, and other senior leaders as necessary.

5. Standard Exceptions

The Chief Information Officer 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. Incident Classification

The following matrix outlines how incidents and disasters will be categorized by the Crisis Assessment and Management Team (CAMT).

Category	Description	Key Determinants
1	Minor disruption to non-critical systems	Expected resolution < 24 hours; no alternate site needed
2	Major disruption; recovery at primary site > 24 hours but feasible	Damage or facility issue; primary data center still usable
3	Total outage of multiple systems; alternate site faster	Major facility disruption; extensive damage; recovery > 72 hours
4	Total loss of data center; recovery time unknown	Data center destroyed or unsafe; full relocation required

7. Service Criticality and Restoration Alignment

A-State ITS aligns institutional CAMT incident classifications with ITS technical restoration priorities to ensure a unified, risk-based recovery sequence.

Institutional Criticality Category Alignment

Category	Description	Example Functions
1 – Critical (Immediate)	Essential to life safety, financial integrity, core academic operations, and communications.	Receiving funds, student registration and grading, transcript production, VoIP, email, and web presence.
2 – Priority (24–72 hours)	Important; delays beyond 24–72 hours significantly affect operations or compliance.	Procurement and disbursement, admissions processing, student account changes, and ISIR loads.
3 – Important (72+ hours)	Tolerates longer outages without major institutional risk.	HR and Financial Aid tasks, Alumni/Development, and lower-impact departmental operations.
4 – Non-Critical	Minimal impact; restore after Categories 1–3.	Departmental servers and low-impact web or class servers.

Note: Criticality may vary at significant times on the university calendar, including the first week of a semester, final exam week, or fiscal year end.

Mapping to Technical Restoration Priorities

ITS Priority	Mapped Institutional Category	Examples from Inventory
Priority 1	Category 1	Active Directory, DNS forwarders, VMware clusters, SAN management, VoIP Call Managers, E911, Exchange CAS/Mailbox, and Banner integrations.
Priority 2	Category 2	ISI Billing, Campus Receivables Collector, Ethos production, Banner XE Solutions Manager, and Doc-Image.
Priority 3	Category 3	CommServ/Syslog, wireless controllers, test environments, and secondary AD/DC nodes.
Priority 4	Category 4	Departmental servers, Mailman, KACE client management, and VDI non-essential components.

The full restoration inventory with system owners and contacts is maintained in the **Restoration Priorities** register, IRP Appendix B. During an event, CRT restores Priority 1 systems first, followed by Priorities 2–4.

Unless otherwise specified in system-specific runbooks, the following target ranges apply:

Recovery Objectives (RTO/RPO)

Category / Priority	Target RTO	Target RPO	Notes
1 / 1	Immediate to 4 hours	≤ 1 hour, or last successful transaction	Life safety and campus-wide communications take precedence.
2 / 2	≤ 72 hours	≤ 4 hours	Sequence ordered by academic and fiscal calendars.
3 / 3	≤ 7 days	≤ 24 hours	Supports rebuild and service hardening activities.
4 / 4	> 7 days, as scheduled	≤ weekly	Planned reintroduction after stabilization.

8. Infrastructure Redundancies and Failover

Arkansas State University maintains infrastructure redundancy and failover capabilities to support business continuity and disaster recovery objectives and to minimize the impact of infrastructure disruptions. The campus network is designed with dual cores to increase redundancy and sustain availability during incidents or periods of peak demand.

Critical enterprise services, including ERP, email, identity management, and backup infrastructure, are hosted in resilient cloud environments when available to leverage geographic redundancy and provider-managed failover. Voice and essential communications systems incorporate failover and survivability capabilities to maintain emergency and operational communications during outages.

Where defined by system criticality, contingency compute environments in Azure and Logical Front are available to support service restoration and continuity during prolonged disruptions. Infrastructure redundancy and recovery capabilities are reviewed and tested as part of ongoing BC/DR governance.

9. Backups and Data Protections

A-State implements layered backup and data protection mechanisms for critical infrastructure to support timely restoration following incidents or disruptions. Backup strategies are designed to align with defined recovery objectives and to reduce reliance on single locations, platforms, or technologies.

Standard backup processes, configurations, and retention expectations are documented and maintained in A-State ITS Backup Procedures, which are reviewed and updated annually to reflect current operational practices.

- Short-term on-premises backups for virtual machines and network-attached storage supporting rapid restoration needs. Currently implemented using a seven-day on-premises virtual machine and NAS backup model.
- Immutable offsite backup copies retained for a defined period to protect against data corruption, ransomware, or other destructive events. Currently implemented using a fourteen-day immutable offsite backup solution, such as Wasabi.

- Additional cloud-based backup replicas, maintained where configured, to enhance resiliency and geographic separation. Currently implemented through secondary cloud backup copies, such as Apex3.
- Data migration to institutionally approved cloud collaboration and storage services, where appropriate, to reduce dependency on on-premises storage infrastructure. Currently implemented through migration of NAS data to cloud-based collaboration platforms, such as Microsoft Teams and SharePoint.

Backup configurations represent baseline practices and may vary by system based on data classification, system criticality, architectural design, and risk considerations. Backup integrity and recoverability are validated through restoration testing as part of ongoing Business Continuity and Disaster Recovery governance. This restoration testing is completed in alignment with the testing and training cadence matrix.

10. Cloud Service Considerations

ITS leverages managed and cloud-hosted services to enhance resilience, availability, and disaster recovery capabilities. Critical institutional platforms are delivered through externally hosted software-as-a-service, platform-as-a-service, and infrastructure-as-a-service solutions that provide geographically distributed infrastructure, provider-managed redundancy, and documented disaster recovery capabilities.

11. Restoration Sequence

During an incident, the CRT executes restoration in the following order:

1. **Protect life safety and communication:** Restore VoIP/Call Managers, E911, Active Directory, DNS, email, core virtualization/storage, and essential Banner integrations.
2. **Stabilize academic and financial operations:** Restore Priority 2 systems aligned to the calendar, including procurement, disbursement, admissions/registrar, Campus Receivables, Doc-Image, and Ethos production.
3. **Resume supporting functions:** Restore Priority 3 systems, including secondary AD/DCs, Syslog, wireless, and test environments.
4. **Restore low-impact and departmental resources:** Restore Priority 4 systems, including departmental servers, VDI non-critical components, Mailman, and KACE.

12. Communication

Internal Communication

- Activate the Calling Tree as required based on incident scope and severity.
- Utilize available communication channels, including hotline or voicemail broadcasts, Microsoft Teams, email, and campus web updates.
- Provide status updates to executive leadership and key stakeholders at regular intervals appropriate to the severity and operational impact of the incident, as determined by the Crisis Assessment and Management Team.

External Communication

External communications during incidents will be managed in accordance with the A-State Campus Emergency Action Plan and established institutional processes.

- University Police coordinate emergency response and engagement with external emergency services as required.
- The Office of University Communications serves as the sole authorized point of contact for public statements and media communications.
- Executive leadership is responsible for notifications to external agencies, insurers, regulatory bodies, and institutional partners as applicable.

External communications priorities, timing, and messaging will guide and inform corresponding internal communications to maintain alignment, accuracy, and institutional control during incident response and recovery.

13. Testing, Training, Exercise, and Review

Arkansas State University Information Technology Services maintains a structured and recurring program of testing, training, exercise, and review to validate the effectiveness of business continuity and disaster recovery capabilities.

The following activities are conducted according to the established cadence below, with additional testing performed as warranted by system changes, risk assessments, or significant incidents:

Annual Activities

- Business Continuity and Disaster Recovery tabletop exercises are conducted annually to validate roles, decision-making authority, escalation paths, and internal and external communication coordination.
- Comprehensive After-Action Reviews are completed following annual exercises and any declared major incidents to document lessons learned, identify gaps, and develop corrective action plans. Corrective actions are tracked to completion.

Periodic Technical Testing

- Targeted technical recovery tests for critical enterprise systems, communications infrastructure, ERP data, and cloud-hosted services are conducted on a recurring basis, not less than annually, and may be scheduled more frequently for systems classified as Critical or Priority.
- Backup restoration drills are performed quarterly to validate data recoverability, backup integrity, immutability protections, and alignment with defined RTO and RPO targets.
- Ad-hoc testing may be initiated following major infrastructure changes, migrations, or onboarding of new critical services.

The results of all exercises and tests will be documented and reviewed by the CAMT, with the gap analysis generated from this review being used to improve business continuity and disaster

recovery readiness.

Testing and Training Cadence

Activity	Minimum Requirement	Recommended Requirement	Responsible Party
BC/DR Specific Tabletop Exercise	Annually	Semiannually	Assistant Vice Chancellor of IT Infrastructure and Operations
Backup Restoration Drills - Active Test, Non-ERP	Quarterly	Monthly	Assistant Vice Chancellor of IT Infrastructure and Operations
Backup Restoration Drills - Active Test, ERP	Quarterly	Monthly	Assistant Vice Chancellor of ERP Application Services
Documentation Review	Annually	Semiannually	Assistant Vice Chancellor of IT Infrastructure and Operations

14. Security and Compliance Alignment

Business Continuity and Disaster Recovery planning, execution, and testing activities must align with institutional information security standards and applicable legal, regulatory, and contractual requirements. This includes, but is not limited to, requirements related to criminal justice information, federal financial aid regulations, data protection, and records retention.

Information security controls must remain effective during backup, recovery, alternate processing, and restoration activities to protect the confidentiality, integrity, and availability of institutional data.

15. Monitoring and Enforcement

The Assistant Vice Chancellor of IT Infrastructure and Operations is responsible for monitoring compliance with this Business Continuity and Disaster Recovery Standard across ITS-supported systems and services.

Compliance is assessed through a combination of:

- Annual BC/DR plan reviews and tabletop exercises
- Scheduled technical recovery and restoration testing
- Backup and restore validation activities
- After-Action Reviews following incidents or exercises
- Periodic audits or assessments requested by executive leadership, Internal Audit, or regulatory bodies

The Assistant Vice Chancellor of IT Infrastructure and Operations is responsible for ensuring that systems managed under their purview meet defined recovery objectives, responsible team members participate in required testing, and accurate recovery documentation is regularly

maintained.

Identified gaps, deficiencies, or failures to meet defined BC/DR requirements must be documented and tracked through corrective action plans with assigned owners and target remediation dates. Risks that cannot be remediated within acceptable timeframes must be formally documented and escalated to the CIO.

16. 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

- Technology Resource Management Standard
- Information Technology Services (ITS) Communication & Service Level Agreement (SLA) Standards
- Data Security and Classification Policy
- A-State Campus Emergency Action Plan
- A-State ITS Backup Procedure

2.3 Compliance Framework Implementation and Assurance Standard

Effective Date: July 1, 2026
Revised Date: July 1, 2026

1. Purpose

This document establishes the annual requirements of Arkansas State University (A-State) to maintain and audit adherence to state and federal compliance frameworks. Through the processes outlined in this standard, University staff will be equipped to confirm that effective controls have been implemented and identify potential gaps in existing controls.

2. Scope

This standard applies to all data, personnel, assets, information management systems, and technology resources under the responsibility of Information Technology Services (ITS). Where applicable, specific compliance framework requirements will not be covered in this standard as their responsibility lies outside of ITS. Where these responsibilities fall outside of ITS, they shall be formally documented, assigned to the appropriate business unit, and acknowledged through institutional governance processes.

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.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates, and members of the system community.

Institutional Data - Any data created, collected, maintained, transmitted, or recorded by A-State in support of academic, administrative, research, or operational functions. This includes data used to conduct official university business, regardless of format or storage location, including digital systems, paper records, and cloud services.

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 compliance framework implementation and assurance processes. Ensures that applicable regulatory, statutory, and contractual obligations are identified, translated into actionable controls, and operationalized across institutional systems and processes.

ITS Security Team – Responsible for assisting with ensuring processes outlined in this standard are coordinated and executed regularly. Assists in reviewing major version changes to compliance frameworks and helps inform identified stakeholders within Information Technology Services (ITS) of these changes in collaboration with the CIO. Facilitates the exchange of compliance information with teams across campus outside of ITS.

Security Panel – Responsible for reviewing internally generated audit reports and assisting with the coordination of university audits. Serves as a core component of the incident response process.

Data Custodians (Digital Records) - Responsible for implementing and operating the technical and administrative controls that protect digital institutional data in accordance with applicable compliance frameworks and institutional policy. This includes enforcing authorized access, safeguarding data throughout its lifecycle, and supporting audit, monitoring, and incident response activities.

Data Custodians (Physical Records) – Responsible for implementing and operating administrative and operational controls to protect physical institutional data outside the scope of this policy.

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. State and Federal Compliance Frameworks

As a public higher education entity, Arkansas State University is required to comply with the following compliance frameworks:

- Gramm-Leach-Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- Criminal Justice Information Services (CJIS)
- Title IV
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR)

7. Shared Compliance Controls

While individual compliance frameworks will require unique controls for implementation and assurance, many will have a common foundation of controls. To ensure adherence to the compliance frameworks listed in this standard, Arkansas State University ITS shall:

- Maintain a formal internal audit schedule for each framework. This audit will serve as a self-study of university compliance and will be used to determine gaps for formal remediation. This internal audit shall occur no less than once every 12 months.
- Maintain a formal audit procedure for each compliance framework.
- Establish scope of responsibility for each framework. This will ensure that the correct stakeholders are identified and held accountable for their portion of framework compliance requirements.
- Maintain an attestation of responsibility for the lead stakeholder(s) of each compliance framework. This attestation shall be obtained no less than once every 12 months.
- Draft a final audit report outlining identified gaps and satisfied requirements. This audit report will be limited to ITS’ scope of responsibility and will be provided to other stakeholders upon request. This final audit report will be drafted in cycle with the formal internal audit.
- Maintain a central repository of all compliance framework internal audits.
- Provide full copies of all documentation, findings, and reports supporting framework compliance to external audit entities upon request.
- Audit access to institutional platforms at minimum on an annual basis, including external platforms and internal resources.
- Maintain data classification assignments for institutional data in alignment with the Data Classification and Security Policy and enforce access and transmission requirements to ensure data integrity and security.

8. Gramm-Leach-Bliley Act (GLBA) Controls

This section outlines the unique controls for implementation and assurance of compliance with the Gramm-Leach-Bliley Act (GLBA). Arkansas State University ITS shall:

- Develop, implement, and maintain all controls for GLBA in alignment with the standards for safeguarding customer information rules.
- Maintain a comprehensive map of all data sources, vendors, and services that connect with the Banner / ERP platform.
- Maintain updated contracts with each data source, vendor, and service that connects with the Banner / ERP platform.
- Within each maintained contract, keep up-to-date copies of contract-specific security documentation. At a minimum, this shall include an auditor-validated, independently assessed report attesting to the security practices of the vendor or manufacturer of this resource, such as ISO 27001 certification, SOC 2 report, or FedRAMP packet.
- Review the access of each campus in the Arkansas State University System to the Banner / ERP platform.
- Maintain signed attestations from stakeholders at each campus that current access is appropriate and is the minimum privilege necessary to fulfill their job duties.

9. Family Educational Rights and Privacy Act (FERPA) Controls

This section outlines the unique controls for implementation and assurance of compliance with the Family Educational Rights and Privacy Act (FERPA). Arkansas State University ITS shall:

- Enforce access controls to university information systems as outlined within the Logical Access Security Standard to ensure digital record security.
- Review user access quarterly and remove or adjust access based on role changes, separation, or inactivity.
- Ensure hardware deployed in relevant areas of campus is maintained both in configuration and lifecycle maintenance.

10. Criminal Justice Information Services (CJIS) Controls

This section outlines the unique controls for implementation and assurance of compliance with Criminal Justice Information Services (CJIS). Arkansas State University ITS shall:

- Maintain restricted access control to hardware housing sensitive CJIS-relevant data within the server farm.
- Review user access logs to the server farm weekly.
- Review badge access permissions to the server farm badge readers weekly.
- Ensure all staff with access to the ITS building have active CJIS clearance and complete yearly CJIS training.
- Ensure all visitors within ITS that are not CJIS cleared are always accompanied by a staff member with CJIS clearance.
- Enforce access controls to university information systems at a level greater than or equal to the minimum requirements outlined by CJIS.
- Actively manage university accounts to enforce both least privilege and removal of access when no longer relevant.
- Ensure hardware deployed in relevant areas of campus is maintained both in configuration and lifecycle maintenance.

11. Title IV Controls

This section outlines the unique controls for implementation and assurance of compliance with Title IV. Arkansas State University ITS shall:

- Enforce access controls to university information systems as outlined within the Logical Access Security Standard to ensure digital records are secure.
- Actively manage university accounts to enforce both least privilege and removal of access when no longer relevant.
- Ensure hardware deployed in relevant areas of campus is maintained both in configuration and lifecycle maintenance.

12. Payment Card Industry Data Security Standard (PCI DSS) Controls

This section outlines the unique controls for implementation and assurance of compliance with the Payment Card Industry Data Security Standard (PCI DSS). Arkansas State University ITS shall:

- Maintain a current and comprehensive Cardholder Data Environment (CDE) network diagram reviewed and updated at least annually and upon significant architectural changes.
- Maintain and document segmentation of the university’s Cardholder Data Environment to minimize the scope of relevant traffic.
- Ensure point-of-sale devices managed by ITS connecting to the Cardholder Data Environment are configured appropriately and that their lifecycle is suitably managed.
- Maintain documentation of each point-of-sale device managed by ITS that includes serial number, firmware version, manufacturer, model, and MAC address.
- Coordinate with the Treasurer's Office to provide support in maintaining compliance when such work is within the scope of ITS’ responsibility.

13. Health Insurance Portability and Accountability Act (HIPAA) Controls

This section outlines the unique controls for implementation and assurance of compliance with the Health Insurance Portability and Accountability Act (HIPAA). Arkansas State University ITS shall:

- Maintain a current and comprehensive HIPAA network diagram reviewed and updated at least annually and upon significant architectural changes.
- Maintain and document segmentation of the university’s network to minimize the scope of relevant HIPAA traffic.
- Maintain access control to hardware housing sensitive HIPAA-relevant data within the server farm.
- Review user access logs to the server farm weekly.
- Review badge access permissions to the server farm badge readers weekly.

14. General Data Protection Regulation (GDPR) Controls

This section outlines the unique controls for implementation and assurance of compliance with the General Data Protection Regulation (GDPR). Arkansas State University ITS shall:

- Maintain a comprehensive map of all data sources, vendors, and services that house EU personal data.
- Maintain updated contracts with each data source, vendor, and service that house EU personal data.
- Within each maintained contract, keep up-to-date copies of contract-specific security documentation. At a minimum, this shall include an auditor-validated, independently assessed report attesting to the security practices of the vendor or manufacturer of this resource, such as ISO 27001 certification, SOC 2 report, or FedRAMP packet.
- Maintain signed attestations from stakeholders that current access is appropriate and is the minimum privilege necessary to fulfill their job duties for relevant data sources, vendors, and services.

15. Monitoring and Enforcement

A-State shall monitor university technology resources for gaps and noncompliance in accordance with state, federal, and University regulations and policies. This monitoring includes, but is not limited to, the following:

- Annual review of each compliance framework’s requirements in alignment with the requirements listed in this standard.
- Annual attestations of compliance for each framework listed in this standard shall be maintained.
- A thorough gap analysis will be completed after each audit, and remedial action or compensating controls will be implemented within six (6) months of identification.
- Reported or discovered noncompliance of any framework will trigger an out-of-cycle audit to ensure gaps are addressed in a timely manner.

Enforcement mechanisms include, but are not limited to, the following:

- Disablement of the offending user’s access to relevant institutional data.
- Network containment of noncompliant technology resources.
- Removal of the noncompliant vendor, service, or resource from university information systems and technology resources.
- Discipline in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the applicable Handbook.

16. 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

- Data Security and Classification Policy

2.4 Enterprise Resource Planning (ERP) Standard

Effective Date: July 1, 2026
Revised Date: July 1, 2026

1. Purpose

This standard establishes the mandatory requirements for the management of the Ellucian Banner Enterprise Resource Planning (ERP) system at Arkansas State University (A-State). The purpose of this standard is to ensure this resource is managed in a manner that protects university data and mitigates institutional risk. Through the processes outlined in this standard, University staff will be equipped to manage the institution's ERP system securely and efficiently.

2. Scope

This standard applies to all faculty, staff, students, contractors, affiliates, and members of the Arkansas State University System community who access Arkansas State University's ERP system and associated resources. This standard applies to all institutional data as governed by the Data Security and Classification Policy and applies in all work settings, including on campus, remote work locations, and approved telecommuting arrangements.

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 A-State.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates, and members of the system community.

System Community - Any person who accesses the ASU System's IT infrastructure who is not classified as a member of the faculty, staff, or enrolled student.

Ellucian Banner - The system of record for academic, financial, human resources, and student-related operations across multiple campuses within the institution's ERP ecosystem.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of ERP controls are responsible for supporting the secure and effective management of the university's enterprise resource planning environment.

This includes:

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

Assistant Vice Chancellor/ERP Systems – Responsible for strategic leadership, governance, and operational oversight of the ERP platform, ensuring alignment with institutional objectives, regulatory requirements, and Ellucian best practices. Coordinates with all campuses to manage and approve changes to shared ERP tables and configurations, ensuring consistency, data integrity, and minimal impact across institutions. Enforces standardized change management practices for enterprise-wide ERP components. Provides direct leadership and strategic direction for the ERP Programming team and the DBA team, ensuring clear priorities, accountability, and coordination across technical functions. Serves as the primary liaison between the ERP team and Ellucian Cloud and Customer Service organizations. Coordinates support interactions, escalations, roadmap discussions, and service issue resolution. Moderates and facilitates ERP governance committee meetings.

ITS Banner DBA Team – Responsible for the security, integrity, availability, and operational reliability of the database. Ensures security adheres to the principle of least privilege. Grants users, applications, and integrations database roles, privileges, and access assignments. Serves as the final technical review authority for all database-related integrations prior to connection with the Production environment. Serves as the primary liaison with the Ellucian Cloud DBA team for coordinating Banner and database upgrades, troubleshooting database-related issues and incidents, and facilitating incident response, root-cause analysis, and corrective actions for ERP-related outages or service degradations.

5. Standard Exceptions

The Banner ERP Steering Committee 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 Banner ERP Steering Committee may delegate this authority as necessary but retains overall accountability for exception management and review.

6. Multi-Entity ERP Environment

The Arkansas State University System (ASU System) consists of seven individual campuses that generally operate independently of each other. The Ellucian Banner ERP system is an exception to this, as each campus within the system utilizes this platform as their ERP solution. In a multi-entity environment such as the ASU System with multiple campuses, colleges, and administrative units, standardization is essential to ensure the integrity of critical institutional data. The following sections of this document establish core components of this standardization.

7. ERP Governance Structure

The Banner ERP Steering Committee oversees the Banner system, cross-campus projects, standards, and change management. This Committee is comprised of chairs from each Functional Area User Group (FAUG) representing each module or specialized group within Banner with members from all institutions in the System, as well as Executive Cabinet member representation.

FAUG membership is tracked via a central spreadsheet to ensure each campus has adequate representation, and this spreadsheet is reviewed on an annual basis. The Chancellor from each institution appoints representatives for each group from their campus. The following FAUGs are the representative groups:

- Accounts Receivable
- Admissions
- Finance
- Financial Aid
- Human Resources
- Institutional Research
- Registrar
- Academics
- Executive Cabinet Members

This committee meets twice a month to discuss Banner service tickets, project status reports, integrations, upgrade, patch and/or release testing, and upcoming Banner downtimes. Each of the FAUG groups meets at least once a month to discuss issues, projects, and concerns within their working group. Chairs and vice chairs are elected from this group each year. Governance procedures associated with shared ERP resources, enterprise-wide configurations, and institution-specific ERP management are further defined in the following section.

8. Shared and Institution-Specific ERP Governance

The Ellucian Banner ERP environment within the Arkansas State University System contains both enterprise-wide shared resources and institution-specific configurations, tables, processes, and data elements. Governance responsibilities for these components are managed differently to ensure both institutional flexibility and enterprise-wide data integrity.

Shared ERP Tables and Enterprise-Wide Configurations

Shared ERP tables, enterprise-wide configurations, and system structures that impact multiple institutions within the ASU System shall be governed through the established Functional Area User Group (FAUG) and Banner ERP Steering Committee governance processes.

Proposed modifications to shared ERP tables or enterprise-wide configurations must:

- Be communicated to impacted FAUG representatives and relevant stakeholders.
- Include sufficient documentation describing the purpose, scope, impact, and implementation requirements of the proposed change.
- Be reviewed through the applicable governance process prior to implementation.
- Receive formal approval through the established FAUG review and voting process before changes are promoted to the Production environment.

Temporary elevated access required to implement approved shared table modifications shall be granted only for the duration necessary to complete the approved change and shall be removed following implementation.

Institution-Specific ERP Tables and Configurations

Arkansas State University is responsible for the governance, management, accuracy, and integrity of institution-specific ERP tables, configurations, business rules, security roles, and operational data elements assigned to the A-State campus environment.

Institution-specific ERP changes at Arkansas State University are typically coordinated and managed by the designated technical lead within the applicable functional area and/or directly by the designated Data Steward responsible for that operational domain.

Institution-specific ERP changes must:

- Comply with institutional data standards and governance requirements.
- Follow established ERP change management and security procedures.
- Be implemented in a manner that does not negatively impact shared ERP resources, enterprise-wide integrations, or other ASU System institutions.
- Be coordinated with the ITS Banner DBA Team when changes could impact integrations, reporting, security, or enterprise-wide operations.

9. Data Ownership and Stewardship

The Ellucian Banner ERP system is organized into discrete functional application areas, such as Student, Finance, Human Resources, and Financial Aid. Each functional area contains institutional

data which supports critical academic, administrative, and operational processes. Institutional data within Banner is owned by the institution as a whole. Data ownership establishes accountability for how data is defined, used, protected, and shared, but ownership does not imply day-to-day management of the technical system.

Directors of each Banner functional area per campus serve as the designated Data Steward for their respective domain. Data Stewards are responsible for ensuring that the data within their functional area is accurate, appropriate, secure, and used in alignment with institutional policies, regulatory requirements, and business needs. Each Data Steward is accountable for:

- Approving access to data within their area based on documented business needs, in coordination with ITS and consistent with the principle of least privilege.
- Ensuring data usage complies with institutional policies, contractual obligations, and applicable laws and regulations, including FERPA, financial reporting requirements, and HR regulations.
- Reviewing all new releases and completing functional testing to ensure that practices and new technologies are being used appropriately within the ERP system.
- Participating in governance and change management processes related to shared tables, configurations, business rules, and integrations that impact their functional area.
- Working with ERP technical teams, governance committees, and other Data Stewards to address cross-functional data dependencies and enterprise-wide impacts.

10. Data Standardization Requirements

All system entities accessing and utilizing the Banner ERP system are required to comply with institutional data standardization requirements. These requirements ensure data within the ERP system is accurate and reliable across shared and individual tables. The ITS Banner DBA team shall maintain a supplemental ERP Data Standards procedure, separate from this standard, which outlines how this data is maintained and input.

11. ERP Integration Deployment and Access Provisioning

ERP integration requests are received by the ERP programming team. Each request must identify the business purpose, data requirements, vendor information, and intended system interactions. Once the request is received, a Banner Programmer is assigned and completes an Integration Worksheet. The programmer also verifies the receipt of appropriate security forms from the vendor, including VPAT and SOC 2 or other approved independent security documentation as outlined in the Technology & Digital Service Purchase Pre-Authorization Procedure.

The programmer will collaborate with the requesting area and vendor to:

- Identify data flows and integration touchpoints.
- Define required data elements and structures.
- Determine transmission and receipt methods, such as APIs, batch processes, or file transfer.
- Ensure alignment with Banner architecture and standards.

All data requests are reviewed to confirm compliance with institutional data standards, security requirements, and applicable regulatory obligations. Integrations must minimize data exposure and comply with the principle of least privilege. If the integration uses or modifies shared tables, approval by the FAUG via formal vote is required before the integration may be promoted to the Production environment.

All integrations, regardless of shared table usage, are distributed to FAUG members for informational awareness to ensure transparency and cross-functional visibility. Integrations must be fully developed and tested in an approved non-production environment prior to Production submission. Testing must validate functionality, data accuracy, security controls, and performance impact. After successful testing, the integration is submitted to the DBA Team. The DBA Team will perform the final technical and security review, verify database impact and controls, and, once approved, deploy to the Production environment.

12. ERP Change Management and Patch Management

All Banner ERP changes must follow a centralized change management process to reduce the risk of data loss or damage to the integrity of system data. As an extension of this change management process, a patch management process must be followed to ensure institutional data does not become corrupted or overwritten by regular and emergency platform patches. The ITS Banner DBA team shall maintain a supplemental ERP Change and Patch Management procedure, separate from this standard, which outlines how these alterations are processed.

This procedure will, at a minimum, establish the following requirements:

- Patches, system upgrades, or other vendor releases must be obtained from trusted sources such as approved vendors.
- Testing of all applied patches, upgrades, and change management procedures is required to ensure effectiveness and reduce potential side effects.
- Patching or upgrading major systems that could impact a substantial number of campus users must be completed during scheduled maintenance windows unless an emergency maintenance window is required due to the criticality of the patch or upgrade.
- Communication to functional users, including patch or upgrade documentation, will be sent with timelines for testing, validation, and Production cutover dates and times.

13. Data Classification

For the purposes of compliance with the Data Security and Classification Policy, all data within the Banner ERP system will be classified as Regulated due to the sensitivity and wide range of data housed within the system. The following requirements outlined for Regulated data apply to this ERP system:

Data Transmission Requirements

- Confidential and Regulated data shall be encrypted during transmission using IT organization-approved cryptographic protocols and configurations. Unencrypted transmission of Confidential or Regulated data is prohibited unless explicitly authorized as

a documented exception.
- Institutional data shall only be transmitted using IT organization-approved systems, services, and communication channels. The use of personal email accounts, consumer file-sharing services, or unapproved messaging platforms for transmitting Internal, Confidential, or Regulated data is prohibited.
- When transmitted via email or messaging systems, Confidential and Regulated data shall be protected through approved technical controls, such as encryption or secure delivery mechanisms, prior to transmission.
- Institutional data classified as Confidential or Regulated shall not be transmitted via insecure protocols, open wireless networks without protection, removable media without encryption, or other mechanisms that bypass institutional security controls.

Artificial Intelligence (AI) Requirements

- Institutional data classified as Confidential or Regulated shall not be entered into, uploaded to, processed by, transmitted through, or otherwise exposed to any Artificial Intelligence (AI) system, service, model, agent, or automated processing technology unless explicitly authorized and approved by the relevant Data Steward and CIO.
- The use of publicly accessible AI platforms to process Confidential or Regulated institutional data is prohibited unless the platform has been formally reviewed and approved by the university for such use cases and appropriate contractual, security, privacy, and data handling safeguards are in place.
- Any approved AI implementation involving Confidential or Regulated data must adhere to institutional requirements related to access control, encryption, retention, logging, monitoring, and third-party risk management.
- Any use of AI must adhere to all requirements outlined in the Artificial Intelligence Governance Standard.

14. Compliance Framework Requirements

All system entities accessing and utilizing the Banner ERP system are required to comply with institutional, state, federal, and accreditation requirements. These include, but are not limited to, the Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), and data retention regulations as outlined in the Records Retention Standard.

This standard establishes the following audit cadence for both direct Banner ERP access and access to platforms that integrate with the Banner ERP system:

- Direct Banner ERP access shall be audited no less than once per year.
- Platforms that integrate with the Banner ERP system shall have their access audited no less than once per year.

15. ERP Security

Security for the Banner ERP and select third-party systems or integrations which interact directly with Banner are administered by the centralized Banner DBA team. Each campus has data owners within the module(s) of Banner who are responsible for requesting and approving security support

within their area for their campus. Requests for a user to be assigned the security role are made to the DBA team via email to its_dba@astate.edu. All access to Banner follows the principle of least privilege.

Service accounts, integration accounts, database accounts, API accounts, and other non-person user accounts used to connect to Banner or Banner-related resources must be requested, approved, provisioned, reviewed, and disabled in accordance with the Logical Access Security Standard. These accounts must be tied to a documented business purpose, assigned to an accountable owner, limited to the minimum access required, and used only for the approved integration or system function.

Shared or generic use of service accounts is prohibited unless explicitly approved as a documented exception. Credentials, keys, tokens, or other authentication methods associated with service accounts must be securely stored, rotated as required, and protected from unauthorized disclosure. Service accounts must be included in the annual Banner ERP access review and reviewed when the related integration, vendor relationship, or business process changes.

16. ERP Incident Response

To ensure adherence to industry standards, the ITS Banner DBA team will maintain, support, and centrally coordinate an ERP Incident Response process with the institutional goal of reducing operational and cybersecurity risk associated with functional, technical, and security incidents. The ITS Banner DBA team shall maintain a supplemental ERP Incident Response procedure, separate from this standard, that outlines how incidents should be reported, categorized, investigated, communicated, and reviewed.

Incidents involving Confidential or Regulated data must also be escalated and managed in accordance with the institutional Incident Response Plan and applicable breach notification requirements.

17. ERP Backup and Recovery Requirements

The Ellucian Banner ERP environment at Arkansas State University is hosted and managed through Ellucian Cloud services. Backup, replication, recovery, and infrastructure continuity operations are managed by Ellucian in accordance with contractual obligations, service level commitments, and applicable security and operational standards.

Arkansas State University ITS personnel are responsible for coordinating with Ellucian regarding recovery operations, validating service restoration following incidents, and ensuring institutional business continuity requirements are addressed through appropriate governance, vendor management, and incident response processes.

As part of the institutional Risk Assessment and Vendor Management Standard, Arkansas State University shall review applicable Ellucian security and compliance documentation on at least an annual basis, including SOC 2 reports and other relevant independent audit, security, privacy, and compliance attestations provided by the vendor.

18. 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

- Artificial Intelligence Governance Standard
- Data Security and Classification Policy
- Logical Access Security Standard
- ERP Incident Response Procedure
- ERP Data Standards Procedure
- ERP Change and Patch Management Procedure
- Incident Response Plan
- Records Retention Standard
- Risk Assessment and Vendor Management Standard
- Technology & Digital Service Purchase Pre-Authorization Procedure

2.5 Network Security Standard

Effective Date: July 1, 2026
Revised Date: July 1, 2026

1. Purpose

This Standard establishes the mandatory requirements for the management of network resources and network infrastructure at Arkansas State University (A-State). The purpose of this standard is to ensure that these resources are managed in a manner that protects university data and mitigates institutional risk. Through the processes outlined in this standard, University staff will be equipped to manage institutional network resources and network infrastructure at every stage of their lifecycle within A-State.

2. Scope

This standard applies to all faculty, staff, students, contractors, affiliates, and members of the Arkansas State University System community who access Arkansas State University information technology infrastructure and associated resources. This standard applies to all network infrastructure components such as wired and wireless networks, devices, systems, servers, and applications that are connected to the university's network and applies in all work settings, including on campus, remote work locations, and approved telecommuting arrangements.

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 A-State.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates,

and members of the system community.

System Community - Any person who accesses the ASU System’s IT infrastructure who is not classified as a member of the faculty, staff, or enrolled student.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of controls necessary to ensure the effective management and coordination of network security controls. This includes:

Chief Information Officer (CIO) - Responsible for the executive sponsorship, governance, and oversight of the University’s network security processes within the scope of this standard. Ensures that applicable regulatory, statutory, and contractual obligations are identified, translated into actionable controls, and operationalized across institutional systems and processes.

Assistant Vice Chancellor of IT Infrastructure and Operations – Provides strategic leadership for enterprise IT infrastructure and operations, ensuring secure, reliable, and scalable services aligned with institutional goals. Oversees networking, systems, cloud, data centers, and IT security while managing budgets, vendors, governance, and risk.

ITS Networking Team – Designs, implements, and maintains the university’s wired, wireless, and wide area network infrastructure to ensure secure, reliable, and high-performance connectivity across academic, administrative, residential, and public environments. Manages network hardware, services, data center and cloud connectivity, monitoring performance, capacity, and availability while implementing security controls in coordination with ITS Security. Supports new construction and technology initiatives, maintains network standards and documentation, and participates in incident response and on-call support for critical network services.

ITS Security – Responsible for establishing and maintaining the university's IT security program. Responsible for ensuring institutional data, systems, and networks are monitored for cybersecurity threats, vulnerabilities, and unauthorized access. Ensures that identified incidents are assigned to the appropriate responsible party for remediation.

5. Standard Exceptions

The Chief Information Officer 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. Network Infrastructure

The A-State network infrastructure ensures the security, availability, and integrity of institutional data. The primary components responsible for these requirements are the firewall and the dual network core, which are designed to align with the Arkansas State Cybersecurity Standards and Act

504.

Perimeter Firewalls: Firewalls are deployed at strategic points in a high-availability pair to control traffic between internal and external networks. Specific throughput requirements and connectivity patterns are maintained in the A-State Network Standard Operating Procedures to ensure alignment with current institutional demands.

Access Control and Least Privilege: Firewalls utilize Access Control Lists (ACLs) to permit only necessary traffic by default. All firewall rule changes require formal approval before implementation.

Logging and Monitoring: In accordance with state recommendations and institutional security practices, firewall logs must be reviewed on a defined and recurring basis to identify potential security threats, unauthorized activity, configuration issues, or policy violations. At a minimum, automated monitoring and alerting should occur continuously where supported by the platform, with formal manual reviews conducted no less than weekly by ITS personnel based on platform responsibility.

High-risk events, critical alerts, and indicators of compromise should be reviewed daily or in near real-time as feasible and should be reported by the responsible party to the IT Security team when the identified risk is a security incident.

Findings requiring action must be documented, escalated, and tracked through established ITS incident response procedures.

Dual Network Core: The university maintains a redundant dual-core infrastructure to provide high availability and support campus-wide traffic.

Redundancy: Core devices are geographically distributed across campus to ensure continuity in the event of a localized incident.

Connectivity: The core supports industry-standard Link Aggregation (LAG) and provides high-speed fiber connectivity to every building on campus.

Performance: Core hardware is selected to perform simultaneous routing and switching at scales sufficient to handle all campus internet and internal traffic.

Note: For specific hardware specifications, link speeds, and physical installation locations, please refer to the Internal Network Infrastructure Appendix. This ensures the security standard remains current as technology evolves.

7. Use of Network Infrastructure

Arkansas State University invests in substantial and sufficient resources to acquire and operate information technology assets, such as hardware, software, and Internet connections. ITS has a responsibility to manage its resources in the most efficient and effective manner possible and in compliance with all laws, regulations, and sound business practices, while at the same time

protecting and preserving the right to academic freedom. Effective management of these resources will assure students, faculty, and staff adequate access to information and technology over the long term and ensures compliance with Arkansas State University System policy.

Examples of appropriate and inappropriate uses of network infrastructure include, but are not limited to, the following:

Appropriate Use of Network Infrastructure

- Accessing the Internet for work-related research and information gathering.
- Conducting approved research activities in compliance with university policies, grant requirements, and applicable regulations.
- Supporting teaching and learning activities, including course delivery, instructional design, and student engagement.
- Utilizing the network in approved telecommunication services such as Cisco Webex, Jabber, Microsoft Teams, or Zoom.

Inappropriate Use of Network Infrastructure

- Users must not share credentials or allow others to access resources using their unique accounts.
- Users may not physically tamper with networking infrastructure, including Wireless Access Point removal or modifying or removing physical network cabling.
- Users may only access computer accounts that have been authorized for their use.
- Users may only use accounts for their authorized purposes. This restriction shall not prevent informal communication, but resources must not be used for private consulting or personal gain without ASU System General Counsel approval.
- Use in violation of civil or criminal law or regulation at the federal, state, or local levels is prohibited.
- Use in violation of the Arkansas State University System Appropriate Use of Information and Technology Resources is prohibited.
- Use in violation of the Arkansas State University student, faculty, or staff handbooks, as applicable, is prohibited.

Violations of this standard may result in disciplinary action in accordance with Arkansas State University System policies, up to and including revocation of network access, disciplinary action under applicable faculty, staff, or student handbooks, termination of contracts, and/or legal action.

8. Firewall Configuration

To ensure compliance with university standards, the ITS Networking Team will maintain, support, and centrally administer university-owned firewalls with the institutional goal of reducing operational and cybersecurity risk associated with utilizing these resources. The ITS Networking Team shall maintain a supplemental Firewall Management Procedure, separate from this standard, that outlines how these resources are requested to be changed, configured, monitored, recorded for audit purposes, and managed.

This procedure will, at a minimum, include and establish the following requirements:

- Default-deny rule: block all incoming traffic unless explicitly allowed.
- Encryption for traffic where possible, such as using TLS for web traffic.
- Strong security policies for remote access, such as VPN and secure protocols like SSH.
- Regular updates and patches to firewall software and firmware.

9. Network Segmentation

Arkansas State University utilizes network segmentation to isolate certain types of traffic and ensure the security of sensitive data types. The following networks are segmented and isolated:

- **Academic Network** - Used by students, faculty, and staff for routine academic activities.
- **Administrative Network** - Contains sensitive financial, HR, and student information and utilizes stricter access controls.
- **Guest Network** - Isolated from the main network to provide internet access for visitors while limiting access to internal systems.
- **Cardholder Data Environment (CDE)** - Used for university point-of-sale devices and other resources that process cardholder data. Isolated from the main network to reduce the scope of PCI DSS auditing requirements.
- **Research Network / HIPAA** - Contains sensitive research and HIPAA information and utilizes stricter access controls.

10. Remote Access

Remote access to the university network will require approved VPN or Zero Trust Network Access (ZTNA) connections with strong authentication methods, including Multi-Factor Authentication (MFA), and all traffic must pass through firewalls for inspection and protection.

11. Patch Management

To ensure compliance with university standards, technology resources shall be actively patched for system and security updates. ITS will maintain, support, and centrally administer a patch management system with the institutional goal of reducing cybersecurity risk associated with unsupported or out-of-date operating systems. ITS shall maintain a supplemental Technology Resource Vulnerability and Patch Management Standard, separate from this standard, that outlines how technology resource patch versions are maintained.

12. Network Monitoring, Logging, and Auditing

To ensure compliance with university standards, the ITS Networking Team will create and maintain a procedure that encompasses network monitoring, logging, and auditing processes. This procedure shall outline how all network security logs are collected and stored for devices such as firewalls, IDS, and IPS.

This procedure will include and establish, at a minimum, the following requirements:

- How all network logs are stored securely and monitored in real time by the responsible ITS team to detect and respond to incidents.
- Network logs will include VPN authorization attempts, firewall alerts, and other relevant security alerts.
- Network logs must be retained in accordance with the university's data retention policy. Any attempts or successful deletion of logs or disabling of log collection must be documented and reported.

13. Incident Response

To ensure compliance with university standards, ITS will maintain, support, and centrally coordinate a formal Incident Response process with the institutional goal of responding to IT operational and IT security incidents. ITS shall maintain a supplemental Incident Response Plan, separate from this standard, that outlines how the IT organization would respond to an IT security incident or emergency.

14. Bring Your Own Device (BYOD) Management

To ensure compliance with university standards, personal technology resources shall have restrictions and controls separate from those outlined in this standard. ITS will maintain, support, and centrally administer these controls with the institutional goal of reducing operational and cybersecurity risk associated with BYOD equipment. ITS shall maintain a supplemental Bring Your Own Device (BYOD) Governance Standard, separate from this standard, that outlines how these resources are managed.

15. 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

- Bring Your Own Device (BYOD) Governance Standard
- Arkansas Code § 5-71-215 (Computer-Related Crime)
- Firewall Management Procedure

2.6 Risk Assessment and Vendor Management Standard

Effective Date: July 1, 2026
Revised Date: July 1, 2026

1. Purpose

This standard establishes the mandatory requirements for assessing, managing, and monitoring risk associated with third-party vendors that conduct business with Arkansas State University. The purpose of this standard is to ensure that vendor relationships are managed in a manner that protects university data and mitigates institutional risk.

2. Scope

This standard applies to all university personnel involved in the procurement, implementation, renewal, or management of third-party vendors that access institutional data, systems, or services. This includes all individuals that are involved with the onboarding, renewal, or management of a third-party vendor that accesses university information, systems, or services. This standard also applies to all vendor contracts regardless of the vendor size or duration of the contract.

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.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates,

and members of the system community.

Vendor - Any third-party entity that stores, processes, transmits, or has logical or physical access to university data, systems, or network resources.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of controls necessary to ensure the effective management and remediation of technology resource vulnerabilities. This includes:

Chief Information Officer (CIO) - Responsible for the executive sponsorship, governance, and oversight of the University's risk assessment and vendor management processes within the scope of this standard. Ensures that applicable regulatory, statutory, and contractual obligations are identified, translated into actionable controls, and operationalized across institutional systems and processes.

IT Security Team – Responsible for reviewing, classifying, and auditing vendors to ensure alignment with the University's risk assessment and vendor management processes. Assists vendor managers in ensuring existing and new vendors meet minimum security requirements.

ITS Budget Team – Responsible for creating, maintaining, and reviewing vendor contracts within TDX. Works closely with the IT Security Team and contract owners to ensure contracts have updated security documentation.

Data Custodians – Responsible for implementing and operating the technical and administrative controls that protect institutional data in accordance with applicable compliance frameworks and institutional policy. This includes enforcing authorized access, safeguarding data throughout its lifecycle, and supporting audit, monitoring, and incident response activities.

Contract Owner – Responsible for ensuring ongoing compliance with this standard and with any applicable audit or regulatory frameworks. The contract owner will be the primary point of contact for the vendor and is responsible for vendor outreach and proper pre-authorization request submissions. Responsible for obtaining updated security documentation from the vendor in alignment with review cadence.

5. Standard Exceptions

The Chief Information Officer 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. Risk Assessment

All vendor risk must be classified by the IT Security Team when reviewing the initial Technology and Digital Service Purchase Pre-Authorization form, as well as upon contract renewal or yearly review. In accordance with the Data Security and Classification Policy, there are four tiers that data may fall under: Public, Internal, Confidential, or Regulated. These tiers determine the documentation required.

- **Public** – No security documentation is required, but any auditor-validated, independently assessed report attesting to the security practices of the vendor or manufacturer of this resource is preferred.
- **Internal or higher** – An auditor-validated, independently assessed report attesting to the security practices of the vendor or manufacturer of this resource is required for approval, such as a FedRAMP packet, ISO 27001 certification, or SOC 2 report.

Vendor risk is determined by the highest level of data the technology or digital service will access. No contract shall be executed, and no system shall be implemented without completion and approval of the required risk assessment. To undergo a risk assessment, a Technology and Digital Service Purchase Pre-Authorization form must be completed. The procedure and accompanying form can be found within the Technology & Digital Service Purchase Pre-Authorization Procedure.

7. Oversight

The individual listed as the requestor on the Technology and Digital Service Purchase Pre-Authorization form becomes listed as the contract owner once the form is approved and the procurement process is completed. The contract owner is responsible for ensuring ongoing compliance with this standard and with any applicable audit or regulatory frameworks. The contract owner will serve as the point of contact for vendor relationships and will be responsible for procuring updated documentation at the request of the ITS Budget Team or IT Security Team. If applicable, a Data Custodian will be assigned to implement technical and administrative controls.

8. Vendor Review

The Arkansas State University IT Security Team is responsible for the review of all existing and new vendor security practices. When Technology and Digital Service Purchase Pre-Authorization forms are submitted, the IT Security Team reviews the required security documentation to ensure vendor practices and attestations are in alignment with minimum university requirements. This practice ensures that institutional data is managed in a secure manner when outside of institutional control on vendor technology resources.

9. Review Lifecycle

All vendor contracts must be reviewed on an annual basis. Contract owners will be required to submit updated documentation in accordance with this review cadence. Annual review ensures that vendor risk remains within an acceptable threshold for the University and ensures that vendors are compliant with any relevant audit requirements. All vendor risk assessments and required documentation shall be maintained in a centralized repository, such as TDX, in accordance with the ITS Records Retention Standard.

10. Vendor Documentation Management

The ITS Budget Team utilizes the security documentation and information gathered within the Technology and Digital Service Purchase Pre-Authorization form to create an accurate repository of approved and managed resources within TDX. This ensures duplicate requests are identified prior to being worked and simplifies the security review of existing vendors on an annual basis.

11. Compliance and Enforcement

No contract shall be executed until a Technology and Digital Service Purchase Pre-Authorization form has been submitted, the required IT Security risk assessment has been completed and approved, and the procurement process has been finalized. During the annual review, vendors identified as noncompliant must remediate all documented issues within a defined remediation period or obtain an approved exemption. Noncompliance with these requirements may result in termination of system access and denial of contract renewal.

12. 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

- Technology & Digital Service Purchase Pre-Authorization Procedure

2.7 Technology Resource Management Standard

Effective Date: July 1, 2026
Revised Date: July 1, 2026

1. Purpose

This Standard establishes the mandatory requirements for the management of technology resources at Arkansas State University (A-State). The purpose of this standard is to ensure that these resources are managed in a manner that protects university data and mitigates institutional risk. Through the processes outlined in this standard, University staff will be equipped to manage institutional technology resources at every stage of their lifecycle within A-State.

2. Scope

This standard applies to all A-State technology resources that are owned, leased, or managed by the university and that access institutional resources or institutional data. This includes, but is not limited to desktops, laptops, mobile devices, virtual desktops, virtual machines, and specialized computing devices used for academic, research, or administrative purposes.

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 A-State.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates,

and members of the system community.

System Community - Any person who accesses the ASU System's IT infrastructure who is not classified as a member of the faculty, staff, or enrolled student.

Systems Authority - ASU System delegates oversight of particular systems to the head of a specific unit of the ASU System or to an individual faculty member, in the case of technology resources purchased with research or other funds for which he or she is personally responsible.

Systems Administrator - A Systems Authority may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular technology resources.

Certifying Authority - This is the Systems Administrator or other ASU System authority who certifies the appropriateness of an official ASU System document for electronic publication in the course of ASU System business.

Specific Authorization - This means documented permission provided by the applicable Systems Administrator.

Privileged Access – Authorized access that allows a user or account to perform administrative or security-sensitive actions on a technology resource that a standard user cannot perform.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of controls necessary to ensure the effective management of technology resources. This includes:

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

Assistant Vice Chancellor of IT Infrastructure and Operations – Responsible for the management and coordination of the university's patch management program, lifecycle management program, and the technology resource inventory program.

ITS Hardware Services – Responsible for the management and coordination of the university's technology resource repair program. Responsible for the maintenance of technology resource procurement processes such as the generation of purchase orders for campus stakeholders and the maintenance of standard hardware configurations.

ITS Endpoint Technician – Responsible for the management and support of institutional technology resources across the University. This includes the escalation of resources requiring repair, the audit of deployed resources to ensure they comply with standard configuration requirements, and the primary support source of technology resource standard users. Responsible

for the regular inventory of technology resources under their individual responsibility and for updating accurate inventory information in a timely manner when changes occur.

ITS Systems Team – Responsible for the management and configuration of the university's Active Directory Users and Computers (ADUC) and Group Policy environments.

ITS Microsoft Administration Team – Responsible for the management and configuration of technology resource management systems such as mobile device management (MDM) and mobile application management (MAM) solutions.

ITS Security – Responsible for the management and coordination of the university's vulnerability management program and for assisting individual teams with determining sufficient security baselines.

5. Standard Exceptions

The Chief Information Officer 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. Standardized Configuration

To ensure compliance with university standards and a consistent experience for users, all technology resources shall be configured to meet a minimum standard. Both ITS Hardware Services and ITS Endpoint Technicians shall be responsible for ensuring this configuration is complete on all new and existing technology resources under the management of A-State.

This standard configuration shall meet the following requirements:

- Devices shall be named in alignment with the institution's approved naming scheme.
- Devices shall be centrally managed through an approved Mobile Device Management (MDM) platform, such as Microsoft Intune or Jamf.
- Devices shall be joined to the institutional domain, such as Entra or on-premises domains.
- Devices shall display a system use notification to users before granting access to the system. This notification must comply with Criminal Justice Information Services (CJIS) policy v6.0 control AC-8.
- Full disk encryption shall be enabled using an approved encryption standard, such as BitLocker with TPM 2.0.
- Local administrator privileges shall be restricted as follows:
  - Standard users shall not have standing local administrator rights.
  - Privileged access shall be limited to authorized A-State ITS personnel.
  - Authorized privileged access shall not be granted via the use of static local accounts and will instead utilize an approved privileged access management (PAM) solution, such as Microsoft Local Administrator Password Solution (LAPS). Upon use, this password will automatically be regenerated.

- Automatic screen lock shall be enforced after no more than five (5) minutes of inactivity.
- An institutionally approved endpoint detection and response (EDR) solution, such as CrowdStrike, shall be installed and actively reporting to the central management console.
- Technology resources will be configured to restrict security level 3 accounts from direct access. Instead, privileged access shall be granted via elevation from a security level 2 account using system-specific solutions, such as Sudo or RunAs.

7. Standard Noncompliance

Failure to comply with the requirements detailed in this standard increases institutional risk and will result in corrective action being taken. This corrective action includes restriction of access to institutional systems, removal of the technology resource from the network, and/or referral to the appropriate university office for further disciplinary action. Noncompliance may be identified through technical controls, such as access logs and vulnerability scanning, routine audits, or reports from technology resource users and administrators. Suspected noncompliance should be reported to ITS through established support and incident reporting channels.

8. Technology Resource Repair

All institutionally owned technology resources requiring repair may only be repaired through either institutionally approved vendors or by certified Hardware Services staff. Institutionally owned technology resources are not authorized for repairs or servicing by any unapproved third-party provider. All technology resource repairs shall be coordinated by Hardware Services to ensure all restrictions and requirements are met.

Assets requiring repairs or servicing that cannot be completed by certified Hardware Services staff must have full disk encryption enabled using an approved encryption standard, such as BitLocker with TPM 2.0. Any technology resources unable to be encrypted prior to repair must have their storage mechanism removed and securely stored until the resource is returned to institutional control.

9. Standardized Hardware Configuration

To ensure compliance with university standards, a consistent experience for users, and ensure the efficacy of internal hardware repair practices, all newly procured technology resources must be purchased from a limited selection of hardware configurations. ITS shall maintain a list of approved hardware configurations for each major operating system, including Windows, Linux, Mac, and ChromeOS, and will only utilize this standard list when processing purchase requests from departments.

Exceptions to this procurement restriction may be granted on a case-by-case basis and only if the university’s business needs truly cannot be met on one of the available hardware configurations. These exceptions are separate from the CIO exception requirements listed in this standard and are instead the responsibility of the ITS leadership responsible for generating purchase orders of technology resources.

Hardware configurations of variable components such as RAM, storage space, and other minor components of a vendor's hardware configuration that may be changed during the ordering process are not subject to this requirement.

10. Lifecycle Management and Inventory Tracking Requirements

To ensure compliance with university standards, technology resources shall be managed throughout their full lifecycle, from acquisition through disposal. ITS will maintain and administer asset lifecycle management processes, including inventory tracking, assignment, maintenance, and secure decommissioning, with the institutional goal of reducing operational, financial, and security risks associated with unmanaged or improperly disposed technology resources.

These lifecycle management processes will be maintained separately from any other university departments or staff responsible for campus inventory practices. This separation ensures that accurate and actionable information is always maintained and available for ITS staff in both lifecycle management and user support processes. Data produced by this separate inventory will be made available to other university departments or staff responsible for campus inventory practices upon request but otherwise operates independently from their purview.

This lifecycle management will include the following requirements:

- Devices shall be recorded in the institutional technology resource asset inventory and shall be reviewed and validated at least annually, no less than once every 12 months.
- Devices recorded in this institutional technology resource asset inventory will have the following details documented:
  - Device ownership.
  - Device status, including Active, Storage, Lost, Stolen, Repair, or M&R.
  - Assigned data classification.
  - Zone of support from ITS endpoint technicians.
  - Make, model, H-tag, and serial number.
  - Date of procurement and anticipated date of retirement, based on the applicable number of years following procurement date.
  - Purchase order requestor as a fallback identification point.
- Detailed Marketing and Redistribution (M&R) processes will be established and maintained.
- Detailed processes for the secure destruction and disposal of institutional data housed within technology resources in alignment with their assigned data classification will be established and maintained.

11. Patch Management

To ensure compliance with university standards, technology resources shall be actively patched for system and security updates. ITS will maintain, support, and centrally administer a patch management system with the institutional goal of reducing cybersecurity risk associated with unsupported or out-of-date operating systems. ITS shall maintain a supplemental Technology Resource Vulnerability and Patch Management Standard, separate from this standard, that outlines how technology resource patch versions are maintained.

12. Vulnerability Management

To ensure compliance with university standards, technology resources shall be actively monitored for vulnerabilities. ITS will maintain, support, and centrally administer a vulnerability detection system with the institutional goal of reducing cybersecurity risk associated with globally reported and documented vulnerabilities. ITS shall maintain a supplemental Technology Resource Vulnerability and Patch Management Standard, separate from this standard, that outlines how technology resource vulnerabilities are maintained.

13. Export Control

To ensure the security and integrity of institutional technology resources travelling abroad, all assets exiting the country must go through a formal export control process that verifies and approves this travel based on federal travel advisory level. While export control processes are not managed by ITS, the review and configuration of devices travelling falls within ITS responsibilities. IT Security reviews assets and grants approval based on the following matrix:

Travel Advisory Levels	Institutional Tier	Required Application(s)	Required Configuration(s)
Level 1 & 2	3	• CrowdStrike Sensor installed and operational. • Malwarebytes installed and operational.	• Asset correctly assigned to the traveler within TDX. • Asset joined to the institutional domain / MDM enrolled and managed. • Operating system is not EOL. • Asset storage drive encrypted. • Operating system patch is up to date. • All Critical vulnerabilities identified on the asset must be remediated.
Level 3	2	• CrowdStrike Sensor installed and operational. • Malwarebytes installed and operational.	• Asset correctly assigned to the traveler within TDX. • Asset joined to the institutional domain / MDM enrolled and managed. • Operating system is not EOL. • Asset storage drive encrypted. • Operating system patch is up to date. • All Critical and High vulnerabilities identified on the asset must be remediated.
Level 4	1	Institutional assets, assigned or loaned, are not authorized for travel.	Institutional assets, assigned or loaned, are not authorized for travel.
Alternate / High-Risk	1	Institutional assets, assigned or loaned, are not authorized for travel.	Institutional assets, assigned or loaned, are not authorized for travel.

14. Software and Application Control

To ensure compliance with university standards, technology resources shall have their software and applications actively managed. ITS will maintain, support, and centrally administer a software and application management system with the institutional goal of reducing operational and cybersecurity risk associated with rogue or unmanaged software and applications. ITS shall maintain a supplemental Technology Resource Software and Application Governance Standard, separate from this standard, that outlines how software and applications are maintained.

This standard will include the following requirements:

- Software and applications available for installation must be restricted to authorized sources and/or ITS-approved application catalogs.
- Approved software and applications shall be made available to standard users via an institutional mobile application management (MAM) solution, such as Microsoft Company Portal.
- Requests for new software or applications to be purchased and deployed must first be approved through institutional procurement processes.

15. Bring Your Own Device (BYOD) Management

To ensure compliance with university standards, personal technology resources shall have restrictions and controls separate from those outlined in this standard. ITS will maintain, support, and centrally administer these controls with the institutional goal of reducing operational and cybersecurity risk associated with BYOD equipment. ITS shall maintain a supplemental Bring Your Own Device (BYOD) Governance Standard, separate from this standard, that outlines how these resources are managed.

16. 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

- Logical Access Security Standard
- Technology Resource Vulnerability and Patch Management Standard
- Technology Resource Software and Application Governance Standard
- Bring Your Own Device (BYOD) Governance Standard
- Data Security and Classification Policy

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

2.9 Technology Resource User Education Standard

Effective Date: July 1, 2026
Revised Date: July 1, 2026

1. Purpose

This standard establishes the mandatory requirements for the management of technology resources at Arkansas State University (A-State). The purpose of this standard is to ensure that these resources are managed in a manner that protects university data and mitigates institutional risk. Through the processes outlined in this standard, University staff will be equipped to manage institutional technology resources at every stage of their lifecycle within A-State.

2. Scope

This standard applies to all faculty, staff, students, contractors, affiliates, and members of the Arkansas State University System community who access Arkansas State University information technology infrastructure and associated resources. This standard applies to all institutional data as governed by the Data Security and Classification Policy and applies in all work settings, including on campus, remote work locations, and approved telecommuting arrangements.

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 A-State.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates, and members of the system community.

System Community - Any person who accesses the ASU System's IT infrastructure who is not classified as a member of the faculty, staff, or enrolled student.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of controls necessary to ensure the effective management and coordination of technology resource user education. This includes:

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

Employee Training & Development Authority – Responsible for the coordination of mandatory user training requirements, assignment, and record maintenance outlined in this standard.

ITS Helpdesk – Responsible for the development and maintenance of ITS' primary documentation repository and education of users who reach out to tier 1 support staff. Provides ad hoc technology resource training on a requested and scheduled basis.

ITS Security – Responsible for the coordination of institutional technology resource tabletop exercises and phishing campaigns. Provides ad hoc security training on a requested and scheduled basis.

5. Standard Exceptions

The Chief Information Officer 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. Documentation Repository

ITS shall maintain a centralized knowledge base to support self-service learning and consistent guidance across the university. This knowledge base will include the following:

- IT Helpdesk Knowledge Base articles
- Getting-started guides for major systems and applications
- Arkansas State University IT policies and standards
- System usage guidance
- Security best practices

- Common troubleshooting and FAQ resources

Documentation in this knowledge base shall be reviewed and updated annually to ensure the content accurately reflects system changes and new services available to university users.

7. Contacting the ITS Helpdesk

Users may request assistance via ticketing system, email, phone, or in-person support. Support hours are published on the university website.

Users can request assistance through multiple methods, which may include:

- Online ticketing system
- Email support – itshelpdesk@astate.edu
- Phone support – 870-972-3933
- In-person support location: Dean B. Ellis Library – Room 149
- In-person support hours: Monday-Friday, 8:00 a.m.-5:00 p.m.

8. Ad Hoc Training Sessions

Information Technology Services offers various supplemental training sessions throughout the year. These trainings are open to all students, faculty, and staff that feel the content is relevant to their job duties and educational experience.

At times, IT Security may assign phishing training when a user interacts with scheduled phishing campaigns. These non-malicious campaigns help prepare users for when they receive a real threat and allow short informational training to be assigned following a user interacting with this “fake” phish.

IT Security also accepts requests from departments to hold customized training sessions depending on their needs. This training can be requested via the Department Training Request form.

To find and attend pre-scheduled ad hoc training sessions, users can view these upcoming events on the university calendar or by viewing their listings on the Daily Digest. Examples of past training topics include:

- Phishing, Social Engineering and Scam Detection
- Cybersecurity Fundamentals and Data Protection
- Formstack virtual training session
- Secure Document Sharing Process Training

9. Criminal Justice Information Services (CJIS) Training

Individuals with authorized access to Criminal Justice Information Services (CJIS)-protected information are required to complete annual CJIS-specific training, as mandated by the Federal Bureau of Investigation (FBI).

This includes, but is not limited to:

- UPD personnel
- All ITS staff with access to data center systems that store or transmit CJIS-related data
- Any other staff or contractors with direct or indirect CJIS system access

CJIS training must be completed annually, in accordance with the FBI's CJIS Security Policy, and records of completion will be maintained for audit and compliance purposes.

10. Artificial Intelligence (AI) and Automated Decision Tool (ADT) Training

In alignment with the Artificial Intelligence Governance Policy, the Arkansas State University System shall develop a training program for all students, faculty, staff, and users of the system concerning the appropriate use of artificial intelligence and automated decision tools in deciding an outcome in the course of their time as an authorized user of the system's technology resources. This training shall be included in all new employee and student training and will be completed on an annual basis.

11. Annual Employee Compliance Training

At the recommendation of the ASU System Office and our Board of Trustees, A-State has implemented a series of required monthly training courses for employees. These trainings reinforce our shared commitment to professionalism, safety, compliance, and a supportive campus environment.

At the start of each month, users will receive an email from training@AState.edu with instructions for accessing the assigned course(s) through the Employee Learn Center.

12. Tabletop Exercises

To support user awareness and reinforce required security practices, Information Technology Services will conduct periodic tabletop exercises. These exercises provide scenario-based discussions that help users understand expected behaviors during security or operational incidents. Participation requirements will be communicated in advance and may include faculty, staff, or designated departmental representatives as appropriate.

Each exercise will document the scenario, participant decisions, identified gaps, and required follow-up actions to ensure continuous improvement of institutional processes and user readiness.

13. Key Performance Indicator (KPI) Monitoring

To ensure the efficacy of user education materials, Information Technology Services shall monitor certain metrics such as phishing simulation failure rates or relevant disciplinary events. KPI monitoring is intended to ensure consistent application of this standard and to identify opportunities for improvement. In the execution of this goal, ITS shall complete the following:

- Conduct periodic phishing simulations.
- Track user susceptibility metrics.
- Report trends to leadership.
- Adjust training programs based on risk indicators.
- Provide additional targeted training sessions for areas identified at risk.

14. 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

- Artificial Intelligence Governance Policy

2.10 Vulnerability and Patch Management Standard

Effective Date: July 1, 2026
Revised Date: July 1, 2026

1. Purpose

This Standard establishes the mandatory requirements for assessing, managing, and monitoring risk associated with vulnerabilities and operating system patches on Arkansas State University technology resources. The purpose of this standard is to ensure that these risks are managed in a manner that protects university data and mitigates institutional risk.

2. Scope

This standard applies to all Arkansas State University employees who work to manage or oversee Arkansas State University technology resources. This includes all individuals that directly report to the central Information Technology Services department and any systems authority who has been delegated access to maintain a technology resource.

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.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates, and members of the system community.

System Community - Any person who accesses the ASU System's IT infrastructure who is not classified as a member of the faculty, staff, or enrolled student.

Systems Authority - ASU System delegates oversight of particular systems to the head of a specific unit of the ASU System or to an individual faculty member, in the case of technology resources purchased with research or other funds for which he or she is personally responsible.

Systems Administrator - A Systems Authority may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular technology resources.

Certifying Authority - This is the Systems Administrator or other ASU System authority who certifies the appropriateness of an official ASU System document for electronic publication in the course of ASU System business.

Specific Authorization - This means documented permission provided by the applicable Systems Administrator.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of controls necessary to ensure the effective management and remediation of technology resource vulnerabilities. This includes:

Chief Information Officer (CIO) - Responsible for the executive sponsorship, governance, and oversight of the University's vulnerability and patch management processes within the scope of this standard. Ensures that applicable regulatory, statutory, and contractual obligations are identified, translated into actionable controls, and operationalized across institutional systems and processes.

Assistant Vice Chancellor of IT Infrastructure and Operations – Responsible for the management and coordination of the university's patch management program, lifecycle management program, and the technology resource inventory program. Responsible for ensuring ITS Endpoint Technicians and ITS Systems Team remediate identified vulnerabilities in the required timeframes.

IT Security Team – Responsible for configuring, maintaining, and coordinating the effective management of vulnerabilities on university technology resources. This includes the identification of applicable vulnerabilities, including insufficient patch versions, and communicating the relevant data to the party responsible for remediation.

ITS Endpoint Technician – Responsible for the remediation of identified vulnerabilities and insufficient patch versions on university technology resources in alignment with SLA standards and remediation timelines outlined in this standard.

ITS Systems Team – Responsible for the remediation of identified vulnerabilities on university infrastructure, such as servers, in alignment with SLA standards and remediation timelines outlined in this standard.

Systems Authority / Delegated Authority – Responsible for the remediation of identified vulnerabilities on university technology resources outside the management of Information Technology Services (ITS) in alignment with the SLA standards and remediation timelines outlined in this standard.

5. Standard Exceptions

The Chief Information Officer 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. Target Remediation Timelines

All identified vulnerabilities and misconfigurations shall be targeted for remediation in alignment with the following timelines. This timeline will be set based on the criticality of the vulnerability with an enhancement based on potential data classification impact.

Tier	Low	Medium	High	Critical
Public	180 Days	180 Days	90 Days	30 Days
Internal	180 Days	90 Days	60 Days	30 Days
Confidential	90 Days	45 Days	30 Days	14 Days
Regulated	30 Days	14 Days	7 Days	24-48 Hours

Remediation timeline and classification are set by the Arkansas State University IT Security Team at the time of remediation assignment. Excessive noncompliance with the targeted remediation timeline may result in the technology resource(s) being removed from the university network.

Vulnerabilities that are compensated for by another control or that have their risk accepted by the CIO shall be tracked and documented via the vulnerability management platform's suppression rules or other comparable mechanism.

7. Vulnerability Management

To ensure compliance with university standards, technology resources shall be actively monitored for vulnerabilities. The IT Security Team will maintain, support, and centrally administer a vulnerability detection system with the institutional goal of reducing cybersecurity risk associated with globally reported and documented vulnerabilities.

This vulnerability management will include the following requirements:

- The authority to manage and administer Arkansas State University's vulnerability management program is delegated solely to the IT Security Team by the CIO. The CIO maintains full authority and executive oversight of this program despite this delegation.
- Any technology resource owned by Arkansas State University or connecting to Arkansas State University's network will be subject to vulnerability scanning as warranted by the IT Security Team.
- Failure to remediate an identified vulnerability within the outlined timeline on any technology resource owned by Arkansas State University or connecting to Arkansas State University's network may result in the removal of the system or device from the network without notification.
- Compliance reviews of Arkansas State University's vulnerability management program will be regularly conducted.
- Users not listed within the responsibilities section of this standard will be prohibited from viewing or accessing detailed vulnerability scan results for systems and/or devices in which they do not have a need to know.
- Users not listed within the responsibilities section of this standard will be prohibited from running vulnerability detection applications on or against systems for which they have not been approved.
- For the purposes of data classification, any information or scan results detailing sensitive security flaws within Arkansas State University's technology resources will be considered confidential.
- IT Security shall establish and maintain automated reports or publish dashboards to relevant users listed in the responsibilities section to assist with the preventative remediation of vulnerabilities prior to a formal communication being sent out by IT Security.

8. Vulnerability Remediation

Identified vulnerabilities will be communicated to the group responsible for remediation based on the responsibilities outlined in Section 4 of this document by the IT Security Team. This communication shall use the following communication methods:

Tier	Low	Medium	High	Critical
Public	Team Dynamix Ticket (P4)	Team Dynamix Ticket (P4)	Team Dynamix Ticket (P4)	Team Dynamix Ticket (P4)
Internal	Team Dynamix Ticket (P4)	Team Dynamix Ticket (P4)	Team Dynamix Ticket (P4)	Team Dynamix Ticket (P3)
Confidential	Team Dynamix Ticket (P3)	Team Dynamix Ticket (P3)	Team Dynamix Ticket (P3)	Team Dynamix Ticket (P2) & Direct Email
Regulated	Team Dynamix Ticket (P3)	Team Dynamix Ticket (P2) & Direct Email	Team Dynamix Ticket (P2) & Direct Email	Team Dynamix Ticket (P1) & Direct Email

Failure to remediate an identified vulnerability within the outlined timeline on any technology resource owned by Arkansas State University or connecting to Arkansas State University's network may result in the removal of the system or device from the network without notification.

9. Patch Management

To ensure compliance with university standards, technology resources shall be actively patched for system and security updates. The Assistant Vice Chancellor of IT Infrastructure and Operations will maintain, support, and coordinate a centrally administered patch management system with the institutional goal of reducing cybersecurity risk associated with unsupported or out-of-date operating systems.

This patch management will include the following requirements:

- The authority to manage and administer Arkansas State University's vulnerability management program is delegated solely to the Assistant Vice Chancellor of IT Infrastructure and Operations by the CIO. The CIO maintains full authority and executive oversight of this program despite this delegation.
- Any technology resource owned by Arkansas State University will be subject to these patch management practices as warranted by the Assistant Vice Chancellor of IT Infrastructure and Operations.
- Patches, system upgrades, or other vendor releases must be obtained from trusted sources such as approved vendors or other external parties.
- Testing of all applied patches, upgrades, and change management procedures are required to ensure effectiveness and reduce potential side effects.
- Patching or upgrading major systems that could impact a substantial number of campus users must be completed during regular maintenance windows unless an emergency maintenance window is required due to the criticality of the patch or upgrade.
- Failure to patch or update a technology resource in a timely manner may result in its removal from the Arkansas State University infrastructure without notification for the protection of other technology resources and institutional data.

10. 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

- Technology Resource Management Standard
- Information Technology Services (ITS) Communication & Service Level Agreement (SLA) Standards
- Data Security and Classification Policy

2.11 Logical Access Security Standard

Effective Date: July 1, 2025
Revised Date: July 1, 2026

1. Purpose

This Standard establishes the mandatory requirements for account creation, management, and information system management across all technology resources and accounts within Arkansas State University (A-State). The purpose of this standard is to ensure that accounts and access controls are managed in a manner that protects university data and mitigates institutional risk.

2. Scope

This standard applies to all faculty, staff, students, contractors, affiliates, and members of the Arkansas State University System (ASU System) community who access A-State information technology infrastructure and associated resources. This standard applies to all institutional platforms and services and applies in all work settings, including on campus, remote work locations, and approved telecommuting arrangements.

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 A-State.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates,

and members of the system community.

System Community - Any person who accesses the ASU System's IT infrastructure who is not classified as a member of the faculty, staff, or enrolled student.

Systems Authority - ASU System delegates oversight of particular systems to the head of a specific unit of the ASU System or to an individual faculty member, in the case of technology resources purchased with research or other funds for which he or she is personally responsible.

Systems Administrator - A Systems Authority may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular technology resources.

Certifying Authority - This is the Systems Administrator or other ASU System authority who certifies the appropriateness of an official ASU System document for electronic publication in the course of ASU System business.

Specific Authorization - This means documented permission provided by the applicable Systems Administrator.

Privileged Access – Authorized access that allows a user or account to perform administrative or security-sensitive actions on a technology resource that a standard user cannot perform.

Access Control (Logical Access Control) - The administrative and technical measures used to identify and authenticate a user or system and then authorize, enforce, and audit the level of access that identity is authorized for based on least privilege and business need. This includes, but is not limited to, username and password, Multi-Factor Authentication mechanisms, and role or group-based authorization, such as RBAC.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of controls necessary to ensure the effective management and security of digital institutional data. This includes:

Chief Information Officer (CIO) - Responsible for the executive sponsorship, governance, and oversight of the University's information systems management processes within the scope of this standard. Ensures that applicable regulatory, statutory, and contractual obligations are identified, translated into actionable controls, and operationalized across institutional systems and processes.

IT Security Team – Responsible for monitoring the campus' digital infrastructure for both internal and external threats and verification of compliance with organizational objectives and regulatory requirements. This includes the investigation and response of reported or identified security incidents and maintenance of monitoring tools.

ITS Systems Team - Responsible for the campus' domain-level system administration. Responsible for designing, documenting, maintaining, and overseeing enterprise infrastructure, system configurations, and access to control frameworks. This includes the active management and documentation of all information system accounts.

ITS Endpoint Technicians - Responsible for the management and support of institutional technology resources across the University. This includes the audit and remediation of deployed resources to ensure they comply with standard configuration requirements, the appropriate use of elevated or standard accounts, and the primary support source of technology resource users.

5. Standard Exceptions

The Chief Information Officer 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. Passphrase Requirements

This section of the standard serves to establish four account security levels and outline their respective passphrase requirements. These account security levels serve to accommodate varying account passphrase requirements based on the sensitivity of systems accessed. Universal account passphrase requirements apply to all security levels unless specified otherwise. This section also outlines requirements for local account passphrases but does not place them at a specific security level as their use outside of emergencies is explicitly restricted.

Account Classification Matrix

Security Level 1 Accounts	Security Level 2 Accounts	Security Level 3 Accounts	Security Level 4 Accounts
Student Accounts	System Administrator Security Level 1 Accounts	System Administrator Accounts	Service Accounts
Faculty Accounts	CJIS User Accounts		
Staff Accounts			
CUI User Accounts			
Shared Accounts (Exception only)			

Passphrase settings are not considered enforced unless systematically required.

6.1 Universal Account Passphrase Requirements

Prohibited Passphrases:
Passphrases must not appear on known compromised passphrase lists or commonly used

passphrase databases. Passphrases will be screened against such lists during passphrase creation and change. A mechanism will be used to detect user passphrases that become compromised after being selected by the user.

Passphrase Reuse:

- A user's passphrase cannot match their last 24 set passphrases within the campus' information systems.
- Users must create unique passphrases for each individual system to which they are given access.
- Reuse of personal account passphrases for business purposes is strictly prohibited.

New User Passphrases:
Users will be required to change their initially assigned passphrase.

Multi-factor Authentication:
Users will be required to authenticate using a multi-factor solution during their first authentication of the day for each individual resource. This authentication will be valid for a period of four (4) hours. Security Level 3 and 4 accounts are excluded from this universal requirement and will instead follow a stricter requirement as outlined in their section.

Alternative Authentication Solutions:
Other technologies for user identification and authentication, such as biometrics, including fingerprint verification or signature verification, and use of hardware tokens, such as smart cards, will be considered and made available for users, if appropriate. Security Level 3 and 4 accounts are excluded from this universal requirement and will instead follow a stricter requirement as outlined in their section.

Duplicated Passphrases:
All user passphrases will be unique and cannot match the passphrase of another account in the campus' information system. This includes any additional account a user may have, such as an administrator account, but excludes accounts synced to the same passphrase using passphrase synchronization at the domain level.

6.2 Security Level 1 Accounts

Passphrase Length:
Account passphrases must be a minimum of 15 characters in length.

Passphrase Complexity:
Passphrases must include at least one uppercase letter, one lowercase letter, one number, and one special character. Repetitive or sequential characters, such as "aaaaaa" or "1234abcd," cannot be present.

Passphrase Rotation:
Account passphrases will expire after a period of 365 days. This expiration will force the user to set a new account passphrase on their next login attempt.

Account Lockout Threshold:
Accounts will be temporarily disabled for 15 minutes after five (5) consecutive failed attempts within a 15-minute period. At the end of this 15-minute lockout, the user's account will automatically unlock, and the process will restart. Passive authentication attempts are excluded from this requirement.

6.3 Security Level 2 Accounts

Passphrase Length:
Account passphrases must be a minimum of 20 characters in length.

Passphrase Complexity:
Repetitive or sequential characters, such as “aaaaaa” or “1234abcd,” cannot be present. No other complexity requirements are imposed.

Passphrase Rotation:
Account passphrases will expire after a period of 365 days. This expiration will force the user to set a new account passphrase on their next login attempt.

Account Lockout Threshold:
Accounts will lock after five (5) consecutive invalid logon attempts by a user during a 15-minute period. This account will stay locked until an A-State representative releases the account. Passive authentication attempts are excluded from this requirement.

6.4 Security Level 3 Accounts

Passphrase Length:
Account passphrases must be a minimum of 20 characters in length.

Passphrase Complexity:
Repetitive or sequential characters, such as “aaaaaa” or “1234abcd,” cannot be present. No other complexity requirements are imposed.

Passphrase Rotation:
Account passphrases will expire after a period of 365 days. This expiration will force the user to set a new account passphrase on their next login attempt.

Account Lockout Threshold:
Accounts will lock after five (5) consecutive invalid logon attempts by a user during a 15-minute period. This account will stay locked until an A-State representative releases the account. Passive authentication attempts are excluded from this requirement.

Enhanced MFA Requirements:
Users will be required to authenticate using a multi-factor solution upon each account authentication.

Technology Resource Configuration:
Technology resources will be configured to restrict Security Level 3 accounts from direct access. Instead, privileged access shall be granted via elevation from a Security Level 2 account using system-specific solutions, such as Sudo or RunAs.

6.5 Security Level 4 Accounts

Passphrase Length:
Account passphrases must be a minimum of 30 characters in length.

Passphrase Complexity:
Account passphrases must be sufficiently complex and resistant to brute-force or dictionary attacks. Use of randomly generated passphrases is required.

Passphrase Rotation:
Account passphrases will expire after a period of 730 days. If an employee who has accessed a Security Level 4 account leaves the organization, this passphrase will be reset.

Passphrase Access:
Security Level 4 account information will be stored in a single passphrase management system. Access to passphrases in this system by administrators must be logged with access logs retained for a minimum of three years.

Early Passphrase Rotation:
When an employee who has accessed a service account leaves the organization, that Security Level 4 account passphrase must be reset within 12 hours of the employee's account being disabled. A passphrase reset of this nature will be considered an emergency priority for change management purposes.

7. Local Accounts

In alignment with the A-State Technology Resource Management Standard, local accounts will be restricted as follows:

7.1 Local Account Passphrase Requirements

Technician Generated Accounts

- Local user or administrator accounts created by either endpoint technicians or systems administrators for specific use cases will have their passphrases changed every 60 days. Passphrase age will be tracked within an EDR when available to ensure compliance.
- Account passphrases will be a minimum of 25 characters with at least one uppercase letter, one lowercase letter, one number, and one special character.
- Local user or administrator accounts created by either endpoint technicians or ITS Systems Team must be documented and have an approved CIO exception on file.
- Local user or administrator accounts, other than a system-generated default administrator account, will not be permitted on endpoints in areas such as the University Police

Department, Information and Technology Services department, the University Data Center, and any other area containing Regulated or Confidential data as classified by the Data Security and Classification Policy.

7.2 Local Administrator Privileges

- Standard users shall not have standing local administrator rights.
- Privileged access shall be limited to authorized A-State ITS personnel.
- Authorized privileged access shall not be granted via the use of static local accounts and will instead utilize an approved privileged access management (PAM) solution, such as Microsoft Local Administrator Password Solution (LAPS). Upon use, this password will automatically be regenerated.

8. Passphrase Enforcement and Monitoring Controls

A-State shall maintain a supplemental Logical Access Password Enforcement and Monitoring Procedure, separate from this standard, that outlines the technical controls ITS utilizes for password enforcement and password compliance ensuring this monitoring is maintained in accordance with state, federal, and university regulations and policies. At a minimum, this will include and establish the following subjects:

- How Fine-Grained Passphrase Policies (FGPP) are configured to ensure compliance with this standard.
- How passphrase complexity and length requirements are configured to ensure compliance with this standard.
- How Entra passphrase protection for Active Directory is configured for both on-premises and cloud-based accounts in compliance with this standard.
- How CrowdStrike compromised password workflows are configured to ensure compliance with this standard.

9. Access Management Requirements

To ensure compliance with university standards, the ITS Systems Team will maintain, support, and centrally administer user accounts with the institutional goal of reducing operational and cybersecurity risk. The ITS Systems Team shall maintain a supplemental Logical Access Account Management Procedure, separate from this standard, that outlines how these resources are configured, monitored, and managed.

This procedure will, at a minimum, include and establish the following requirements:

- All user accounts will follow a defined and documented naming scheme.
- Shared accounts are not permitted for access to A-State information systems. Though “shared” by administrators, service accounts are not considered shared accounts for the purposes of this requirement.
- All service accounts will be thoroughly documented by the ITS Systems Team, with purpose and any automated tasks executed defined.

- Information system accounts will be created so that they enforce the most restrictive set of rights, privileges, or accesses required for the performance of tasks associated with their assigned job duties.
- Information system accounts with rights, privileges, or accesses extending into the administrative management of endpoints, information systems, or other technology resources will result in an administrative account being created for the user. This administrative account will exist solely for the completion of assigned job duties extending beyond that of a standard user account.
- All information system accounts will be actively managed. Active management includes the acts of establishing, documenting, activating, modifying, disabling, and removing accounts from A-State's information systems. This work will be completed by a domain-level system administrator.
- Timelines and requirements for the timely disablement of accounts when their assigned user is no longer employed or associated with the organization.
- Information system accounts are to be reviewed by the ITS Systems Team to verify access is still relevant to their assigned duties.

Review will include verification of:

- Continued business justification for access.
- Confirmation of appropriate role-based group membership.
- Any access that is no longer justified must be revoked within one (1) business day of the review.

10. Access Management Controls

Management of A-State access controls shall meet the following requirements:

- Access to information system resources will be logged and stored for a minimum of seven (7) years unless otherwise specified in the University Data Retention Procedure. Suspicious access will be reported to the Security Team for evaluation.
- Service account usernames and passphrase information will be stored, transmitted, and tracked using a single passphrase management solution. Account information is not permitted for transmission via any other form of communication.
- Service account passphrases shall be rotated within 24 hours of the receipt of the termination workflow for any user(s) that have accessed the service account.
- The ITS Systems Team will create adequate documentation of the account management processes, tools, workflows, and mechanisms required to actively maintain A-State access management controls.

11. Use of Access Controls

Arkansas State University invests substantial and sufficient resources to acquire and operate information technology assets, such as hardware, software, and Internet connections. ITS has a responsibility to manage its resources in the most efficient and effective manner possible and in compliance with all laws, regulations, and sound business practices, while at the same time

protecting and preserving the right to academic freedom. Effective management of these resources will assure students, faculty, and staff adequate access to information and technology over the long term and ensures compliance with Arkansas State University System policy. Examples of appropriate and inappropriate uses of access controls include, but are not limited to, the following:

Appropriate Use of Access Controls

- Users only use their assigned user account for access to A-State resources.
- Users only use their assigned authentication methods, such as MFA, to access A-State resources.
- Using university-approved password management solution(s) to store access control information.
- Reporting observed violations of this Logical Access Security Standard.

Inappropriate Use of Access Controls

- Sharing access credentials such as passwords with another user.
- Sharing authentication methods such as access to MFA mechanisms with another user.
- Providing inappropriate access to another user in violation of the principle of least privilege.
- Writing access control information outside of a secure, university-approved password management solution.

12. 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, 2025
Next Review Date: July 1, 2027
Version: 2.0

Referenced Policies, Standards, and Procedures

- Technology Resource Management Standard
- Data Security and Classification Policy
- Arkansas State University Data Retention Procedure
- Logical Access Account Management Procedure
- Logical Access Password Enforcement and Monitoring Procedure

2.12 Records Retention Standard

Effective Date: May 2, 2025
Revised Date: September 2, 2025

---

1. Purpose

This standard establishes the procedures and standards for Arkansas State University in connection with the retention of University records by various divisions and departments of ASU. It is the intent of this procedure to ensure that all University records are maintained in accordance with all applicable statutory and procedure requirements in order to make certain that University records are not improperly or prematurely disposed of by a University department. Additionally, this procedure provides guidance to University employees as to appropriate time frames under which University records that are no longer necessary for the operation of the University may be properly disposed of, thereby promoting efficient and effective use of the University's limited storage capacity.

---

2. Scope

These standards apply to all A-State controlled records listed in appendix A and must be followed by all departments within Arkansas State University.

---

3. Disposal Process for University Records

The delegates of executive custodians identified in the records retention schedule in Appendix A may authorize and subsequently dispose of University records when the retention period for said records has expired. Disposal must be conducted in a manner as identified by the "Disposal Method" and must be documented. The following criteria must be met in order to dispose of applicable records:

1. The records to be disposed of meet or exceed the time frames established for such record s in Appendix A.
2. The disposal of the records complies with statutory, contractual, or accreditation obligations.
3. The records to be disposed of do not relate to or contain information regarding current, pe nding or potential litigation involving the University.

Any questions regarding these criteria should be addressed to the University Legal Counsel through the Vice Chancellor for Finance and Administration.

These criteria do not apply to individual documents that are processed individually as a part of an e mployee's daily activities, but rather to large quantities of records which have been retained as a p art of the University archival and retrieval practices.

---

4. Record Security

The security of physical (printed or microfilmed) records is the responsibility of the respective Executive Custodian, regardless of storage location. The security of electronic records is the responsibility of the enterprise technology services organization - Information & Technology Services (ITS).

---

5. Standard Modification

It will occasionally be necessary to update this standard as statutes, regulations, and business processes change. In the event that modification is necessary, the University data management committee will define and draft modifications to this procedure, for approval by the executive staff of the University.

---

6. Standards Review

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

Effective Date: May 2, 2005
Next Review Date: October 25, 2027
Version: 1.1

Appendix A

This spreadsheet provides a comprehensive, though not exhaustive, listing of official Arkansas State University documents and their associated retention requirements. The retention timelines were last reviewed and updated on **October 25, 2026** by the respective Executive Custodians serving on the University Data Management Committee. This appendix serves as a centralized reference to support consistent records management, compliance, and institutional stewardship across all units.

A-State ITS Records Retention (102526).pdf

Review Cycle

10/25/26 - Updates to records retention document for UPD - addition of security camera retention and updates to other UPD document types. No other substantive changes to standard.

2.13 Institutional Asset and Device Naming Standard

Effective Date: August 13, 2025
Revised Date: September 17, 2025

---

1. Purpose

This document establishes a standardized institutional asset naming convention for all Arkansas State University (A-State) owned devices and applicable technology assets. The goal is to create a clear, consistent, and scalable system for identifying devices based on departmental ownership, type, and operating system, ensuring efficient inventory management, technical support, and integration with enterprise systems such as Microsoft Intune and TeamDynamix (TDX).

---

2. Scope

These standards apply to all A-State owned computers, servers, virtual machines, and other institutional technology assets that are managed, tracked, or supported by Information Technology Services (ITS). This also applies to all assets supported by decentralized campus technicians across administrative and academic departments.

The naming convention **must** be followed by all departments when commissioning, reassigning, or reimaging an institutional device. This standard may also be extended to other asset types (e.g., printers, POS systems) to promote uniformity across the enterprise.

---

3. Responsibilities

All university personnel involved in the provisioning, deployment, and configuration of institutional assets are responsible for following this naming standard. This includes:

- **Hardware Services**: Responsible for ensuring that all newly procured and reimaged devices are named in compliance with the standard before being issued to end users.
- **Campus Technicians**: Required to apply the correct naming convention during on- site setup, troubleshooting, or when reimaging/redeploying devices within their assigned departments or units.
- **Other Authorized Personnel**: Any individuals with delegated authority to configure or rename institutional assets must always ensure compliance with this standard.

Non-compliance with these standards may result in corrective actions, including mandatory renaming of devices and possible audit findings during ITS asset reviews.

4. Naming Convention Schema

All standard device names will follow the structure below:

Department Code – Device Type & OS Code – Serial Number

Where:

- **Department Code**:Uses the official department code list provided in Appendix A. As new departments form, this appendix will be updated by ITS to accommodate this.
- **Device Type Code**:
  - **D** = Desktop
  - **L** = Laptop
  - **S** = Server
  - **K** = Kiosk
  - **V** = Virtual Machine
  - **DS** = Digital Signage
- **Operating System (OS) Code**:
  - **W** = Windows
  - **M** = Mac
  - **L** = Linux
  - *If Device Type Code = DS, Skip adding OS Code.*
- **Serial Number**: Manufacturer's serial number (may be truncated if necessary to meet system name length restrictions). For Apple devices and other platforms with shorter limits, truncation is expected to ensure the full name is 15 characters or fewer.

Example Device Names

- **SYS-DW-2X518M2** → Windows desktop at the ASU System Office
- **ABI-LW-2X518M2** → Windows laptop in the ABI department
- **SYS-DM-H2WGM0LF** → Mac desktop at the ASU System Office
- **ITS-DS-H87UFC8** → Digital Signage in the ITS Building

Note: All device names will be in uppercase. No lowercase characters are allowed.

Note: Device type code for Virtual Machine will be applied if an asset is both a VM and a server.

---

5. Naming Schema Special Considerations

Assets such as virtual machines (VM) and servers may differ slightly in naming scheme when compared to a standard asset such as a desktop or a laptop. Due to the nature of these resources, no serial number is required and can instead be supplemented with additional device information for ease of identification.

All alternative device names will follow the structure below:

Department Code – Device Type & OS Code – Alternative Code

Example Device Names

- **ITS-VL-PV-PD-01** → Linux VM that is an ITS resource. This is a private and production resource.
- **UPD-SW-WATCHGUARD01** → Windows Physical Server that is a UPD resource. It hosts the Watchguard resource and is the first of these servers.

A full list of alternate codes for VM's and Servers can be found in Appendix B of this document.

---

6. Justification for Asset Naming Convention

- **Immediate Identification** – Enables ITS staff and departmental support teams to quickly identify the departmental owner, device type, and operating system, streamlining troubleshooting and support.
- **Simplified Inventory Management** – Reduces complexity in tracking devices across Microsoft Intune, TDX, and other asset management systems.
- **Scalable and Sustainable** – Supports institutional growth without ambiguity, enabling uniform standards across all campuses and departments.
- **Cross-Platform Consistency** – Eliminates naming conflicts and promotes uniform standards, even when devices are managed by different teams.

---

7. Implementation and Compliance

- All new devices entering the institutional asset inventory **must** follow the standard naming format at the time of deployment.
- Existing devices must be renamed to align with the convention during reimaging, reassignment, or major system updates.
- ITS will verify compliance during asset audits and periodic reviews of device inventory in Intune and TDX.
- Devices utilizing the alternate codes laid out in section 5 of this document must have full written documentation, such as a referenceable spreadsheet, of their purpose, criticality, serial number (if not a VM) and functional ownership to be considered in compliance with this standard.
- Exceptions to this standard must be approved in writing by the Chief Information Officer (CIO) or their designee.

---

8. Standards Review

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

Effective Date: August 13, 2025
Next Review Date: August 13, 2026
Version: 1.1

Appendix A – Official Department Codes

The following table lists the approved department codes for use in the naming convention. This list is maintained by ITS to ensure consistency with institutional records.

Department	Department Code
ABI	ABI
Academic Affairs	AA
Academic Diversity	DIV
Access & Accommodation Services	AAS
Accreditation & Assessment	AS
Alumni, Development, University Advancement	ADV
A-State Online Services	AOS
Arkansas Heritage Sites	AHS
Athletic Administration, Compliance, Marketing, Training, Sports	ATH
Campus Card Center	CCC
Career Services	CS
Center for Excellence in Teaching	CET
Chancellor's Office	CHN
Childhood Services	CHS
College of Agriculture	COA
College of Business	COB
College of Education	COE

Department	Department Code
College of Engineering & Computer Science	ENG
College of Liberal Arts & Communications (includes Art, Music, Theatre)	CLA
College of Nursing	NHP
College of Sciences & Mathematics	CSM
Counseling Center	CC
Delta Center for Economic Development	DEL
Digital Creative Media	DCM
Environmental Health & Safety	EHS
Facilities Management	FM
Faculty Center	FC
Finance & Administration	FIN
Financial Aid	FA
FNBA	FNB
Foundation	FND
Fowler Center	FOW
International Programs	OIP
Graduate School	GRD
Heritage Studies	HS
Honors	HON
HOWL	HWL
Human Resources	HR

Department	Department Code
Information Technology Services	ITS
Institutional Research	IR
ITS AV - Classroom devices	AV
ITS - Loaner Devices (For International Travel)	LNR
Library	LIB
Military Science	MIL
Multicultural Center	MC
Museum	MUS
Office of Admissions	ADM
Parking Services	PAR
Procurement Services	FM
Publications & Communications Services	PCS
Red Wolf Center	RWC
Registrar	REG
Research & Technology Transfer	RTT
RESTORE	RES
Sponsored Programs Accounting	SPA
ASU System Office	SYS
Testing Center	TST
University College	UC
University Housing	UH
University Police	UPD

Department	Department Code
Veterinarian School	VET

Appendix B – Alternate Virtual Machine Codes

The following table lists the approved virtual machine codes for use in the naming convention. This list is maintained by ITS to ensure consistency with institutional records.

Code Description	VM/Server Code
Production	PD
Development	DV
Public	PB
Private	PV
The name may vary but will clearly reflect the operational function of this asset.	[SERVER FUNCTION]

2.14 Mobile Hotspot and MiFi Usage Standard

Effective Date: October 4, 2025
Revised Date: October 4, 2025

1. Purpose

This standard outlines the approved use, eligibility criteria, and request procedures for mobile hotspots and MiFi devices managed by Information Technology Services (ITS) at Arkansas State University. MiFi devices are provided to support short-term, mission-critical connectivity needs for university business purposes.

---

2. Scope

This standard applies to all Arkansas State University employees, faculty, staff, and departments requesting temporary mobile internet connectivity via a MiFi device provided by ITS.

---

3. Appropriate Use Cases

MiFi devices are intended for temporary, short-term use in specific, approved situations such as:

- **University Travel**: When an employee is traveling for university business in areas with unreliable or no network connectivity.
- **Remote Instruction Support**: When a faculty member delivering hybrid or online courses lacks sufficient bandwidth from their home internet provider.
- **Short-Term Projects or Events**: When a university-sponsored activity, research project, or outreach event requires temporary internet access in areas without reliable connectivity.

---

4. Inappropriate Use Cases

MiFi devices are **not** to be used as a permanent or general solution for connectivity. Prohibited uses include:

- **Long-Term Connectivity Replacement**: MiFi devices are not substitutes for home or office internet connections.
- **Permanent Departmental Connectivity**: Departments must seek long-term network or ISP solutions rather than rely on MiFi devices.

- **Point-of-Sale (POS) or Institutional Device Use**: Non-cellular devices such as payment systems or kiosks must connect via approved secure wired or wireless networks.
- **Personal Convenience**: MiFi devices are not issued for convenience, preference, or non-business-related access.

---

5. Eligibility Criteria

To be eligible for a MiFi device, the requestor must:

- Demonstrate a temporary, university-related business need.
- Obtain supervisor or department head approval.
- Provide a clear justification outlining the intended purpose, location, and duration of use.

---

6. Request and Approval Process

The following process should be followed to request a MiFi device:

1. **Submit Request**: A MiFi request must be submitted through the ITS Service Portal using the designated TeamDynamix form: MiFi Request Form
2. **Review**: ITS will review the request to ensure it aligns with appropriate use cases and device availability (based on preferred network).
3. **Approval/Denial**: ITS will notify the requestor and supervisor of the decision. Denials will include a rationale and may suggest alternative connectivity options.

---

7. Usage and Return Requirements

The user is responsible for:

- Returning the device promptly at the end of the loan period.
- Ensuring responsible use that complies with all university IT and data security policies.
- Avoiding personal or non-business-related data usage in alignment with Cell Phone and Data Phone Devices Use policy.

Failure to return equipment or excessive non-business use may result in departmental charges.

---

7. ITS Responsibilities

ITS will:

- Maintain and track an inventory of MiFi devices.
- Conduct quarterly audits to verify the status of all MiFi devices by contacting users and departments to confirm whether each device is still needed and actively being used.
- Monitor usage, data limits, and compliance with cellular network provider.

- Provide setup and technical support (liaison with cellular network provider) as needed.

---

8. Standards Review

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

Effective Date: October 4, 2025
Next Review Date: October 4, 2027
Version: 1.0

Review Cycle

9/27/26 - No updates are necessary.

2.15 Electronic Forms Creation & E-Signature Standard

Effective Date: February 25, 2026
Revised Date: February 25, 2026

---

1. Purpose

This standard establishes institutional requirements and approved platforms for the creation, deployment, and management of electronic forms at Arkansas State University (A-State).

The purpose of this standard is to:

- Ensure appropriate platform selection based on data classification and workflow complexity
- Protect institutional data and maintain compliance with regulatory requirements
- Provide governance over limited-license platforms
- Prevent redundant or unsupported form technologies
- Align electronic form development with enterprise architecture standards

---

2. Scope

This standard applies to all academic and administrative departments at Arkansas State University, including all faculty and staff who create, deploy, or manage electronic forms for official university business. It governs the collection of data through public-facing and internal forms, including forms used for operational processes, workflow routing, approvals, authenticated submissions, and legally binding agreements.

This standard applies to any electronic form used to collect, store, or route institutional data on behalf of the university, regardless of audience or intended use.

---

3. Approved Electronic Form Platforms

Arkansas State University maintains a defined set of institutionally approved electronic form platforms to ensure data security, regulatory compliance, accessibility, workflow efficiency, and responsible license management.

The appropriate platform selection is determined by the complexity of the workflow, authentication requirements, data sensitivity, and the need for legally recognized electronic signatures. Departments must use the approved platforms outlined below and select the solution that best aligns with the specific business and compliance requirements of their form use case.

3.1 Formstack (Primary Institutional Platform)

Formstack is the primary approved platform for departmental electronic forms.

Formstack may be used for:

- Public or internal data collection
- Standard administrative workflows
- Approval routing
- Conditional logic and notifications
- Moderate complexity processes

Formstack is the default platform for:

- Departmental operational forms
- Surveys requiring structured data capture
- Standard approval workflows

Departments may create and manage Formstack forms within licensing allocations and ITS governance standards.

3.2 Slate (Enterprise Workflow & CRM Use Case)

Slate may be used for:

- Complex workflows
- CRM-integrated processes
- Admissions-related processes
- High-volume, logic-driven workflows
- Multi-stage process automation

Use of Slate outside of enrollment management workflows must be coordinated with the Data & Technology team within ITS and the Slate administrators. Contact EMDataTech@astate.edu for more information on using Slate to collect form submissions.

3.3 Pack Portal Forms (Authenticated Use Cases)

Pack Portal forms may be utilized when:

- Authentication is required
- The identity of the submitter must be verified
- Data must be tied to institutional identifiers (e.g., name, email, A-State ID)

- Secure routing is required within authenticated sessions

Pack Portal is appropriate for:

- Student-facing authenticated forms
- Employee-specific submission forms
- Institutional record-tied workflows

Contact packportal@astate.edu for more information on using Pack Portal to collect form submissions.

---

4. DocuSign – Restricted Use Cases

A-State maintains limited institutional licensing for DocuSign.

Due to contractual envelope limits and license constraints, DocuSign use is restricted to specific institutional use cases only and must be approved by ITS prior to being used with the A-State enterprise license.

4.1 Approved DocuSign Use Cases

DocuSign may be used only when:

- Federally recognized or legally binding electronic signatures are required, examples include:
  - Athletic coach contracts
  - HR tax documents
  - Official employment documents
- Or, extremely complex, multi-party signature workflows are necessary
- Or, regulatory compliance requires formal e-signature validation – in many cases, the Sign functionality within Formstack may be a viable alternative

4.2 DocuSign Administrative Creation & Governance

Departments are not permitted to independently create administrative DocuSign forms and should follow this process to seek approval.

1. Users must complete the designated TDX request form outlining the business case for DocuSign use.
2. ITS will review the request for:
   - Legal necessity
   - Platform appropriateness
   - Envelope impact
3. Upon approval, the form will be:
   1. Administratively created by ITS

2. Monitored for envelope usage
4. Approved departments will be granted DocuSign viewer licenses to keep track of envelopes and download completed forms as necessary.

DocuSign usage will be centrally tracked to ensure the university remains within contracted volume limits, and ITS reserves the right to determine that an alternative solution may need to be utilized if the annual volume is higher than projected.

---

5. Platform Selection Matrix

The following matrix provides guidance for selecting the appropriate electronic forms platform based on the type of use case, workflow complexity, authentication requirements, and signature needs. Departments should use this table as a reference to ensure alignment with institutional standards.

Use Case Type	**Approved Platform**
Standard departmental data collection	Formstack
Public-facing forms (non-authenticated)	Formstack
Authenticated student or employee form	Pack Portal
CRM-integrated workflow	Slate
Legally binding federal e-signature	DocuSign (Restricted)

---

6. Standards Review

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

Effective Date: February 25, 2026
Next Review Date: February 25, 2027
Version: 1.0