

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

Revision #1

Created 2026-06-26 01:52:41 UTC by Christopher Boothman

Updated 2026-06-26 01:55:44 UTC by Christopher Boothman