

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
-

Revision #1

Created 2026-06-26 01:58:54 UTC by Christopher Boothman

Updated 2026-06-26 02:02:54 UTC by Christopher Boothman