

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

Revision #1

Created 2026-06-26 02:06:43 UTC by Christopher Boothman

Updated 2026-06-26 02:08:56 UTC by Christopher Boothman