Data Security and Classification Policy

Effective Date: October 16, 2026

1. Purpose

The purpose of this policy is to secure and classify all institutional data governed by the Arkansas State University System (ASU System). Along with classifying this data, the policy will also establish appropriate controls to ensure the integrity and security of all institutional data.

2. Scope

This policy applies to all digital data that is managed, stored, and processed by ASU System campuses. This includes data stored on servers, cloud services, endpoints, external storage devices, data warehouses, messaging systems, email systems, and any other digital systems or technology resources, used to store, process, or transmit institutional data.

3. Definitions

- **Technology Resources** – The machines, devices, systems, services, and related components that are used in information processing. This includes the following:
    - Machines, devices, and transmission facilities that are used in information processing, including computers, word processors, terminals, telephones, cables, software, and related products.
    - Devices that are 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 that is related to information processing and wired or wireless telecommunications, including hardware, software, services, planning, personnel, facilities, and/or training.
    - Procedures, equipment, and software that are designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, along with associated personnel, including consultants and contractors.
    - All email accounts that are issued by the ASU System.

- **IT Organization** - The unit at each institution that is responsible for providing information technology solutions and services.
- **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 ASU System community.
- **Systems Authority** – The ASU System delegates oversight of particular technology systems to the head of a specific unit of the ASU System, or to an individual faculty member, in the case of technology resources that were purchased with research or other funds for which they are personally responsible.
- **Systems Administrator** - A Systems Authority may designate another person as "Systems Administrator" to manage the particular system assigned to that individual. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine those persons who are permitted access to particular technology resources.
- **Specific Authorization** - This means documented permission provided by the applicable Systems Administrator.

4. Responsibilities

University personnel who are involved in the configuration, maintenance, and review of controls necessary to ensure the effective management and security of digital institutional data include the following:

- **Chief Information Officer (CIO)** - Responsible for executive sponsorship and oversight of the university's digital data security and classification program. The CIO ensures that appropriate resources, policies, and enforcement mechanisms are in place to support compliance with this policy. The CIO approves risk-based exceptions, resolves cross-unit data security issues, and provides executive accountability for institutional data protection.
- **ERP Team** – Responsible for the configuration, maintenance, and management of university Enterprise Resource Planning (ERP) systems (e.g., Banner).
- **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 for the protection of physical institutional data outside the scope of this policy.

5. Policy Exceptions

The CIO for the campus is authorized to review and approve exceptions to this policy whenever organizational needs justify a deviation, and if the associated risks are deemed acceptable. All exceptions must be documented, including a defined scope, a scheduled review date, and they must incorporate compensating controls when appropriate. The CIO

may delegate this authority, as necessary, but retains overall accountability for exception management and review.

6. Data Classification Matrix

All institutional data shall be identified and classified based on its sensitivity and criticality, as well as the systems that support it. This will ensure that appropriate protection, oversight, and monitoring are applied.

This policy establishes four (4) distinct levels of classification, based on the sensitivity of data and potential regulatory requirements.

Tier	Confidentiality	Integrity	Availability	Examples
Public	Minimal	High	High	Websites and Public Research
Internal	Moderate	Moderate	Moderate	Internal Memos or Procedures
Confidential	High	High	Moderate	FERPA Records, Personnel Files
Regulated	Highest	Highest	High	HIPAA,PCI,CJIS,GLBA

*Please see Appendix A for detailed examples of each data type.

7. Data Classification – Public

Information approved for public release with no expectation of confidentiality. Unauthorized disclosure poses no risk to the university, its operations, or individuals. Public data may be shared freely without restriction.

8. Data Classification – Internal

Information intended for internal university use only. Unauthorized disclosure could cause minor operational, reputational, or administrative impact. Access is limited to authorized university personnel and to affiliates with a legitimate business need.

9. Data Classification – Confidential

Sensitive information that requires protection to prevent significant risk to the university or individuals. Unauthorized disclosure could result in financial loss, legal exposure, reputational harm, or disruption of university operations. While data of this class may cause institutional harm, it does not require mandatory external breach notification.

10. Data Classification – Regulated

Information subject to legal, regulatory, or contractual requirements. Unauthorized disclosure could result in severe financial loss, legal exposure, reputational harm, or major disruption of university operations. Data of this class legally or contractually requires the university to protect the data and to report breaches externally.

11. Records Retention

Each ASU System IT Organization shall maintain a comprehensive Records Retention Standard, separate from this policy, which outlines retention periods, retention locations, data custodians, and disposal methods by type of record. This Records Retention Standard will cover records outside of, and within, the scope of this Data Security and Classification Policy.

12. Data Transmission Requirements

All digital institutional data transmitted across networks, systems, applications, or services shall be protected in accordance with its assigned data classification, in order to prevent unauthorized disclosure, alteration, or interception.

- Data transmission controls shall be commensurate with the data's classification level (Public, Internal, Confidential, or Regulated). **Confidential** and **Regulated** data shall receive the highest level of transmission protection.
- **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, including 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.
- Data transmission activities may be logged, monitored, and reviewed to ensure compliance with this policy, applicable standards, and regulatory obligations. Violations of transmission requirements may result in access revocation or disciplinary action.

13. Data Watermarking Requirements

Each ASU System IT Organization shall maintain classification-based watermarking controls that apply persistent, user-attributable, and non-removable visual markings to **Confidential** and **Regulated** data, in accordance with the data's sensitivity and associated risk. This watermarking requirement will be implemented in alignment with the following table:

Data State	Watermark Applied?	Notes
Data at Rest	No	Encryption Required Instead
File Stored Post-export	Yes	Must Be Embedded before Storage
Display in Web App	Yes (Confidential/Regulated)	Dynamic Overlay Preferred
Printed Document	Yes (Confidential/Regulated)	Mandatory for Regulated
Email Attachment	Yes (if Confidential/Regulated)	Embedded Prior to Send

14. Access Control Requirements

Employees of the ASU System shall be granted access to files, folders, applications, actions, and other data-access methods based on job duties. Access to ASU System data and information systems shall comply with the Logical Access Security Standard.

15. Endpoint Data Security Requirements

The ASU System shall ensure that all endpoints, processing or storing institutional data, are configured to meet the following minimum requirements:

- Devices shall be centrally managed through an approved Mobile Device Management (MDM) platform (e.g., Microsoft Intune).
- Devices shall be joined to the institutional domain or cloud identity service.
- Devices shall be recorded in the institutional asset inventory with documented ownership and assigned data classification. Asset records shall be reviewed and validated at least annually (no less than once every 12 months).
- Full disk encryption shall be enabled, using an approved encryption standard (e.g., BitLocker with TPM 2.0).
- Local-administrator privileges shall be restricted as follows:
    - Standard users shall not have standing local-administrator rights, without specific authorization.
    - Privileged access shall be limited to authorized ASU System Administrators, or their designee(s).
- Automatic screen lock shall be enforced after no more than five (5) minutes of inactivity.
- An institutionally approved endpoint detection and response (EDR) solution (e.g., CrowdStrike) shall be installed, and actively reporting, to the central management console.
- Devices shall comply with the institution's approved software baseline and application control standards.

16. Artificial Intelligence (AI) Requirements

The ASU System shall maintain an Artificial Intelligence Governance Policy, separate from this document, outlining the transparent and responsible use of AI tools on ASU System campuses. This policy shall outline the following requirements relevant to this Data Security and Classification Policy:

- Data, classified as **Confidential** or **Regulated,** is not permitted for entry to any Artificial Intelligence (AI) agent, tool, or processing method, unless explicitly authorized.
- **Internal** data is permitted for entry to AI agents, tools, and processing methods on university-maintained and approved platforms.

17. Policy Review

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

Effective Date: October 16, 2026
Next Review Date: October 16, 2027
Version: 1.0

Referenced Policies, Standards, and Procedures:

- Cloud, Network, and Local Storage Standard
- Logical Access Security Standard
- Endpoint Management Standard
- AI Governance Standard

Appendix A – Data Classification Examples

Please note: This is not an exhaustive list. This appendix is provided to supplement the definitions given in this policy.

Data Type	Classification	Justification
Export Controlled data	Regulated	ITAR, EAR
Credit Card Cardholder Data	Regulated	PCI
Social Security Numbers	Regulated	PII
Donor Financial Records	Regulated	GLBA
Patient Health Records (identifiable)	Regulated	HIPAA
Student Records (non-directory)	Confidential	FERPA
Class Schedules	Confidential	PII
Transcripts	Confidential	FERPA
Personally Identifiable Information	Confidential	PII
Employee Data (not including SSN)	Confidential	Employee privacy
System Security Plans	Internal	Protective information
Unpublished Research Results	Internal	Competitive and commercial potential
Exams (question banks and answer keys)	Internal	Exam integrity
ASU System Directory (students & staff)	Public	FERPA
University Regulations	Public	Intended for public use
Course Catalog	Public	Intended for public use
Public Web Sites	Public	Intended for public use

(Adopted by the Arkansas State University System Board of Trustees on October 16, 2026, Resolution 26-49.)