Other

- 4.1 Acceptable Use of AI Guidelines
- 4.2 Cloud, Network, and Local Storage Guidelines
- 4.3 Cybersecurity Incident Response Plan
- 4.4 Door Access Control and Security Camera Procurement Procedure
- 4.5 ITS Service Commitment & Support Expectations

4.1 Acceptable Use of AI Guidelines

Effective Date: October 22, 2024
Revised Date: August 11, 2025

---

1. Purpose

This document establishes guidelines for the fair, responsible, and ethical use of Artificial Intelligence (AI) by Arkansas State University (A-State) faculty, staff, and students from an IT security perspective. The goal is to ensure that AI is used in ways that align with A-State's academic integrity standards, protect the privacy and security of sensitive data, and support the university's commitment to innovation. These guidelines supplement the ethical use of AI document previously distributed to faculty.

---

2. Scope

These guidelines apply to all A-State employees, students, contractors, and affiliated parties who use AI technologies or tools for academic, research, administrative, or operational purposes. AI tools include, but are not limited to:

- Machine learning applications
- Natural language processing tools
- AI-driven automation software
- Any systems that make decisions or recommendations based on algorithmic data processing

---

3. Definitions

- **Artificial Intelligence (AI):** Technologies that simulate human intelligence to perform tasks or support decision-making. This includes machine learning, natural language processing, and autonomous systems.
- **Acceptable Use:** Ethical and legal use of AI systems consistent with A-State policies and laws.
- **Data Privacy:** Proper handling of personal and sensitive data, including collection, storage, and sharing, in accordance with relevant regulations.

---

4. General Principles

All AI usage at A-State must adhere to the following principles:

- **Transparency and Accountability:**
  Users must disclose when AI is used for decision-making, content generation, grading, or other impactful processes.
- **Bias and Fairness:**
  AI tools must be implemented fairly. Users should actively mitigate biases that may affect individuals based on race, gender, age, or other protected characteristics.
- **Data Privacy and Security:**
  AI usage must comply with A-State data policies and applicable laws, especially those listed in Section 8.
- **Academic Integrity:**
  AI must not compromise academic honesty. Students must disclose AI use where required and follow the Academic Integrity Policy.
- **Informed Consent:**
  Individuals must be informed when their data is processed by AI systems, and explicit consent must be obtained when necessary.

---

5. Use of AI in Education

- **Faculty Responsibilities:**
  Faculty must use AI to enhance—not replace—traditional teaching. They must also disclose AI use in grading and educate students on ethical AI usage.
- **Student Responsibilities:**
  Students may use AI to support learning but must not use it to complete assignments or exams dishonestly.

---

6. Use of AI in Research

AI use in research should:

- Support (not replace) ethical research practices
- Comply with institutional research ethics and regulatory requirements

---

7. Use of AI in Administrative and Operational Functions

When AI is used in university operations (e.g., admissions, financial aid):

- The university must clearly disclose where and how AI is used
- Human oversight must be applied to AI decisions that affect individuals

---

8. Ethical and Legal Compliance

AI use must comply with relevant regulations, including but not limited to:

- **FERPA** (Family Educational Rights and Privacy Act)
- **GLBA** (Gramm-Leach-Bliley Act)
- **HIPAA** (Health Insurance Portability and Accountability Act)
- Other applicable federal, state, or international laws such as:
  - **UK Data Protection Act 2018**
  - **EU GDPR**
  - **EU AI Act**
  - **China's Personal Information Protection Law**

Legal questions should be directed to the ASU System General Counsel's Office.

---

9. Prohibited Uses of AI

The following are not permitted:

- Using AI for academic dishonesty (e.g., cheating or plagiarism)
- Collecting or using personal data without authorization
- Discriminatory or biased use of AI
- AI surveillance without approval from A-State IT Security and Legal departments

---

10. Use of AI Assistant Guidelines

10.1 Overview

AI assistants, such as those integrated into Microsoft Teams or Zoom, can provide valuable support in meetings by generating summaries, action items, and transcripts. However, they 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.

10.2 Risks to Consider

- **Privacy Concerns** – AI assistants record and process meeting content, which may include sensitive or confidential information.
- **Data Security** – Content may be stored in third-party systems depending on the AI service provider, potentially outside the institution's control.
- **Compliance** – Certain discussions (e.g., FERPA-, HIPAA-, or CJIS-protected data) must not be recorded or processed by AI assistants.
- **Informed Consent** – All participants should understand and agree to AI assistant use prior to recording or summarizing a meeting.
- **Legal Considerations** – Recorded discussions and summaries/transcripts may be subject to legal discovery in future litigation.

10.3 Guidance for Approved Use of AI Assistants

- AI assistants should never be enabled by default in recurring meetings or meeting templates.
- AI assistants may be used in Microsoft Teams meetings only when all participants provide explicit consent at the start of the meeting.
- The meeting organizer is responsible for announcing the AI assistant’s presence and its intended function (e.g., transcription, note-taking, summarization).
- Avoid enabling AI assistants in meetings that include confidential, legally protected, or sensitive data.
- Store and share AI-generated notes only in secure, approved A-State storage platforms (e.g., Microsoft OneDrive, SharePoint) and should only be shared with individuals who were part of the meeting.

10.4 General Guidance on Preventing AI Assistants from Joining Meetings

- In Microsoft Teams, review and adjust meeting options before the session to ensure that AI assistants are not automatically admitted.
- Disable transcription, recording, or meeting summarization features unless explicitly needed and approved.
- If an AI assistant joins unexpectedly, the meeting organizer should remove it immediately and verify settings before proceeding.

---

11. Compliance and Enforcement

Misuse of AI may result in disciplinary action per A-State's employee and student handbooks. The university may review AI usage to ensure institutional compliance, especially for licensed tools.

---

12. Review and Updates

These guidelines will be reviewed as AI technologies and regulations evolve. The IT Security Panel will monitor compliance and propose updates when necessary.

---

13. Contact Information

- **Security Inquiries:** security@astate.edu
- **Academic AI Use Questions:**
  Madeline Ragland, Assistant Vice Provost for Academic Student Services
  mprestidge@astate.edu

---

14. Approved AI Platforms

See **Appendix I** for A-State-approved AI platforms. All other tools must go through the standard **Software Purchase Request** process, including submission of a VPAT and HECVAT or ITS Security Questionnaire.

Use of **OpenAI** platforms such as **ChatGPT** or **DALL·E** is discouraged unless a **Business Associate Agreement (BAA)** is obtained.

Appendix I – Approved AI Platforms

The following AI tools meet A-State's compliance and data protection standards:

- **Microsoft Copilot** (Strongly Recommended)
  - Fully compliant with FERPA and HIPAA
- **ChatGPT Business** (requires minimum 2 license purchase by department)
- **Claude Pro** (Anthropic)
- **OtterAI**

While Microsoft Copilot is preferred due to its robust compliance standards, other listed tools are acceptable for use. OpenAI platforms (e.g., ChatGPT, DALL·E) are generally discouraged unless approved through a BAA.

4.2 Cloud, Network, and Local Storage Guidelines

Effective Date: January 28, 2025
Revised Date: February 14, 2025

Purpose

To ensure secure and reliable data management at Arkansas State University, this document outlines guidelines for using cloud storage, network storage (file share), and local storage—focusing primarily on Microsoft OneDrive as the approved platform for storing confidential and internal data.

Scope

These guidelines apply to all A-State employees, faculty, staff, and students who manage, store, or access data using local devices or cloud services.

Definitions

- **Cloud Storage:** Internet-based data storage through a third-party provider, offering flexibility and redundancy.
- **Network Storage (File Share):** Centralized storage managed by ITS on the A-State network, suitable for department-level sharing and automated report delivery.
- **Local Storage:** Files stored on personal computers or external devices without backup or redundancy.

Guidelines

1. Cloud Storage Overview

Cloud storage provides secure, accessible, and backed-up solutions for storing data.

Benefits of Approved Cloud Storage:

- **Accessibility:** Access files from any internet-connected device.
- **Collaboration:** Real-time sharing and co-editing with colleagues.
- **Security:** Meets A-State security standards.
- **Redundancy:** Protects against local device failure.

2. Storage Type Comparison

Storage Type	Key Characteristics	Recommended Use
Cloud Storage (OneDrive)	Secure, backed-up, accessible	Primary solution for confidential/internal data
Local Storage	Not backed up, at-risk of loss	Not recommended for critical data
Network Storage (File Share)	Centrally managed, backed up	For departmental/shared reports, not collaboration

---

3. Approved Storage Services

- **Microsoft OneDrive** *(Primary Cloud Solution)*
  - Meets A-State security standards.
  - Default quota provided; email security@astate.edu to request more.
- **Kaltura** *(Multimedia)*
  - Ideal for large media files (e.g., videos).
- **Canvas LMS**
  - Best for academic course content and storage.
- **Dropbox** *(Limited Support)*
  - Requires case-by-case approval. Migration to OneDrive is encouraged.

---

4. Usage Guidelines

Cloud Storage

- **File Sharing:** Grant access only to necessary individuals. Do not share confidential data externally without approval.
- **Device Sync:** Do not sync confidential data to non-A-State-owned devices.

Local Storage

- Avoid using local devices to store critical or sensitive data. Local data is not backed up and may be lost permanently.

Network Storage

- **Access Control:** Managed by ITS. Access is granted on a need-to-know basis.
- **Use Case:** Ideal for receiving automated reports from systems like Banner or Automic/UC4.
- **Backups:** Regularly backed up by ITS, but not intended for personal or collaborative files.

Roles and Responsibilities

- **ITS Department:** Maintains these guidelines and ensures the use of approved platforms.

- **All Users:** Must adhere to these guidelines to protect university data.

Compliance

Misuse of storage solutions or failure to follow these guidelines may result in violations of the **ASU System Appropriate Use Policy** or other applicable regulations. Compliance is monitored by ITS.

Review and Maintenance

These guidelines are reviewed and updated periodically to stay current with technological and legal developments.

Frequently Asked Questions (FAQ)

1. What is cloud storage?

Cloud storage allows you to store files on the internet using services like OneDrive, enabling secure and remote access.

2. Why is cloud storage important?

It ensures data is backed up, secure, and accessible from anywhere.

3. Can I use Google Drive or other unapproved platforms?

No. Storing confidential or internal data on unapproved platforms may result in data breaches.

4. What’s the risk of local storage?

Local files are not backed up and can be lost due to hardware failure or theft.

5. Why prefer cloud over network or local storage?

Cloud storage provides automatic backup, remote access, and better collaboration. Network storage is for internal, restricted-access reports—not ideal for collaboration or personal storage.

6. Why avoid local storage?

Local devices are not backed up by ITS. Files may be lost permanently in case of failure or damage.

Version History

- **1.0:** Initial document approved – *January 28, 2025*
- **1.1:** Added network storage guidelines – *February 14, 2025*

4.3 Cybersecurity Incident Response Plan

Effective Date: September 17, 2025
Revised Date: October 14, 2026
Responsible Office: Information Technology Services (ITS)

1. Preface

This document and its contents exist to manage and respond to cybersecurity incidents only. Anyone suspecting an exposure of university data or systems should immediately contact:

- **IT Support Services (Help Desk):** 870-972-3933
- **IT Security Team:** security@astate.edu or 870-680-3770

If you are experiencing a non-cybersecurity related security incident and need immediate support, please contact:

University Police Department (UPD): 870-972-2093 (24/7 Dispatch)

Technical access or administrative capability **does not** independently authorize investigation, forensic analysis, disclosure determination, or incident notification.

Staff with administrative access are entrusted with privileged access to university systems, applications, networks, accounts, logs, databases, and institutional information because that access is necessary to administer, maintain, and support university technology resources.

When a potential cybersecurity incident or data breach is suspected, **all** staff, including ITS personnel, should report, preserve, and escalate the matter rather than independently determining whether a breach has occurred, what regulatory or legal requirements apply, whether affected individuals should be notified, or which institutional stakeholders should be involved.

---

2. Purpose

This cybersecurity incident response plan (IRP) provides a comprehensive overview of how Information Technology Services (ITS) staff respond to and recover from identified cybersecurity incidents impacting Arkansas State University Jonesboro (A-State). This IRP identifies and clearly establishes responsibilities during cybersecurity incidents, outlines generic response steps, and ensures institutional data and infrastructure is adequately protected during a true incident.

---

3. Scope

This IRP applies to all data, personnel, assets, information management systems, and technology resources under the responsibility of ITS. Where applicable, specific security incident response plan specifics will not be covered as their responsibility or impact lay outside of ITS and may not be considered a “cybersecurity” incident (e.g., active shooter incident).

This plan also extends to certain members of university leadership outside of ITS (e.g., Chancellors Cabinet, General Counsel, University Communications). Where applicable, the Arkansas State University Police Department (UPD) and the Federal Bureau of Investigation (FBI – Jonesboro Cyber Task Force) will be involved.

---

4. Definitions

- **Cybersecurity Incident** - An occurrence that— (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- **Security Panel** – The individuals responsible for investigating data breaches or other cybersecurity incidents. This panel is comprised of all members of the ITS Senior Leadership and senior members of the IT Security team.
- **Incident Response Coordinator**– The technical lead of the incident response process. Authorizes next steps, including emergency containment actions, and works to ensure adequate resources are made available to other technical staff working on the incident. Ensures the executive lead is adequately informed, and that incident response actions are minimally disruptive to the operations of A-State.
- **Executive Response Coordinator**– The individual responsible for coordinating with university leadership outside of ITS. Provides adequate and timely updates to key stakeholders and works to ensure adequate resources are made available to the security panel in the pursuit of incident response and remediation.

---

5. Responsibilities

All personnel involved in the cybersecurity incident response process. This includes:

- **Chief Information Officer (CIO)** - Responsible for the executive sponsorship, governance, and oversight of the University’s incident response processes within the scope of this plan . Ensures that applicable regulatory, statutory, and contractual obligations are identified , translated into actionable controls, and operationalized across institutional systems and processes. Serves as the executive response coordinator during any true-positive cybersecurity incident.

- **Director of IT Security** – Responsible for the management of A-State's information security program and oversight of the IT security team. Serves as a member of the

security panel and generally as the incident response coordinator during any true-positive cybersecurity incident. Depending on the circumstances of any true-positive incident, other individuals on the security panel may serve as the incident response coordinator .

- **IT Security Team** – Responsible for confirming the validity of reported or alerted cybersecurity incidents. Notifies the security panel upon confirmation of a true positive incident or when an incident cannot be confirmed as false-positive. Provides accurate working data to technical staff and helps to support incident response actions.

- **Security Panel** – Responsible for coordinating technical staff as needed to complete remedial actions during the incident response. Assists with documenting all actions taken and for assisting as necessary with campus coordination.

- **Technical Staff** – Responsible for gathering data from information systems, providing expertise and guidance in technical platforms, the execution of directed remedial actions, and completing adequate documentation of all remedial actions taken at the direction of the security panel.

- **Office of Risk Management** – Responsible for ensuring incident response actions are aligned with the university's overall enterprise risk management framework. Serves as the liaison for institutional cyber liability insurance claims, ensuring required documentation and reporting are completed.

- **General Counsel** – Responsible for advising on legal, regulatory, contractual, evidentiary, and notification obligations related to cybersecurity incidents. Coordinates legal review of external communications and breach notification determinations where applicable.

- **University Communications** – Responsible for coordinating public, campus-wide, media-facing, or stakeholder communications related to cybersecurity incidents, in coordination with the Executive Response Coordinator, General Counsel, and applicable university leadership.

Incident Response Responsibility Matrix

Activity	CIO / Executive Response Coordinator	Director of IT Security / Incident Response Coordinator	IT Security Team	Security Panel	Technical Staff	Risk Management	General Counsel	University Communications
Incident Validation & Escalation	I	R	A/R	I	I	I	I	I
Incident Assessment	I	R	R	A/R	C	C	C	I
Containment	I	A/R	R	R	R	I	I	I
Evidence Preservation	I	A/R	R	R	R	I	C	I
Eradication & Recovery	I	A	R	R	R	I	I	I
Executive Coordination	A/R	C	I	I	I	C	C	C
Legal & Regulatory Review	I	C	I	I	I	C	A/R	I
Public Communications	C	I	I	I	I	I	C	A/R
Post-Incident Review	C	A/R	C	R	C	C	C	I
Key: **R** = Responsible | **A** = Accountable | **C** = Consulted | **I** = Informed								

6. Security Panel Composition

The A-State security panel is comprised of all members of the ITS Senior Leadership and senior members of the IT Security team. This composition ensures that every area is represented in the incident response process and that technical staff from every area are at the disposal of the panel during remedial efforts. This includes:

- Chief Information Officer (CIO)
- Director of IT Security
- Assistant Vice Chancellor of IT Infrastructure and Operations
- Assistant Vice Chancellor/ERP Systems
- Director of Hardware and Communication Services
- Senior Director of Academic Technology and Data Analytics
- Budget Director
- Senior IT Security Analyst
- Security Operations Center Coordinator

---

7. Incident Response Stages

A-State follows a multi-stage incident response process to ensure potential incidents are appropriately vetted and verified before technical resources are assigned to remedial actions. These stages ar e:

- Identification and Confirmation
- Assessment
- Containment
- Eradication and Recovery
- Post-Incident Activity

Given the wide variety of cybersecurity incidents that can occur in an enterprise environment and the need for a concise, easy to follow plan during an incident, these stages will not contain step

by step instructions for each potential incident category.

---

8. Incident Categories and Severity

Incident – Per the Federal Information Security Modernization Act of 2014 (FISMA), as codified at 44 U.S.C. § 3552(b)(2): An occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Major Incident – Per the Office of Management and Budget (OMB) Memorandum M-20-04 or subsequent memo, a major incident is either:

> Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.40 Agencies should determine the level of impact of the incident by using the existing incident management process established in the National Institute of Standards and Technology (NIST) Special Publication (SP) 900-61 Revision 2, Computer Security Incident Handling Guide.

or,

> A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. Major incident determination is required for breaches involving PII of 100,000 or more people .

Breach – Per OMB Memorandum M-17-12 or subsequent memo: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for other than authorized purpose.

Event – Per NIST SP 900-61 Revision 2: An event is any observable occurrence in a system or network.

Vulnerabilities :

- Internal discovery of potential compromise l everaging a vulnerability
- Known exploitation of vulnerability (NVD tagged entries; wide-spread public reporting; viable proof-of-concept exploit released, etc.)

Incident severity will be directly correlated with the classification of the impacted data and the number of users impacted .

Data Classification Tier	Examples	Alternate User Impacted Tier	Incident Severity
Public	Websites and public research	1-250	**Low**
Internal	Internal memos or procedures	251-2 , 500	**Medium**
Confidential	FERPA records, personnel files	2,501-10,000	**High**
Regulated	HIPAA,PCI , CJIS,GLBA	10,001+	**Critical**

---

9. Identification and Confirmation Stage

Upon receipt of an alert or report of a suspected cybersecurity incident, the notified staff should convey all relevant information to the IT security team (security@astate.edu) for review. During this review, the IT security team will work to confirm the validity of the incident and take the following action(s):

- **False Positive Report**
  - Proceed with standard internal procedures depending on the reported incident. Consult with the Director of IT Security if no internal procedure exists.
  - Security panel will not be notified of false positive reports.
- **True Positive or Unconfirmed Report**
  - Escalate the reported incident to the Director of IT Security. If the reported incident is still confirmed as true positive or cannot be confirmed as a false positive, the security panel will be not ified and convene for assessment and remediation.
  - If a reported incident is in the unconfirmed category, it will be treated as a true positive incident by the security panel until otherwise proven false.

When reporting a true positive or unconfirmed report to the security panel, the following information should be provided to expedite the assessment stage:

- What was the initial attack vector?
- Is the threat actor exploiting vulnerabilities to achieve access or privilege?
- Does the threat actor have persistence on the network or device?

- What accounts have been compromised and what privilege level do they have?
- Is this an on-premises , vendor driven, or hybrid incident?

---

10. Assessment Stage

F ollowing the confirmation of a true positive cybersecurity incident, the security panel will be notified and convene to complete an assessment . This assessment will help to gauge the scope of impact and to identify which technical staff need to be allocated to incident containment and eradication / recovery. During this assessment, the following information will be determined :

- System(s) impacted ?
- Is the incident stable, or is the scope continuing to grow?
- What data classification(s) are impacted or at risk? See Data Classification Policy for assistance with identification.
- What campus service(s) are degraded?
- Wh ich technical staff are critical to incident containment?

Prior to moving into the containment phase, the Executive Response Coordinator will notify, at a minimum, the Office of Risk Management to ensure cyber liability insurance requirements are met. Unless otherwise necessary, the CIO will serve as the Executive Response Coordinator.

The final step of the assessment stage is to identify an appropriate Incident Response Coordinator based on the specific details of the incident. Generally, the Director of IT Security will serve in this capacity, but specific incident circumstances may make another member of the Security Panel a more suitable candidate.

---

11. Containment Stage

Following a thorough assessment of the reported cybersecurity incident, the Incident Response Coordinator will begin to leverage all available resources (Security Panel members, technical staff, IT Security team members, etc.) to begin the containment stage. The primary objective of this stage is to prevent further damage to institutional resources and reduce the immediate impact of the incident. The specific approach to containment will vary depending on the type of incident .

Ensure that the containment scope encompasses all related incidents and activity—especially all adversary activity. If new signs of compromise are found, return to the assessment stage to re-scope the incident. Upon successful containment (i.e., no new signs of compromise), preserve evidence for reference or law enforcement investigation, adjust detection tools, and move to eradication and recovery.

Parallel to the containment activities led by the Incident Response Coordinator, the Executive Response Coordinator will be expected to provide an initial communication to campus or other

relevant stakeholders regarding the incident (if appropriate at this stage).

---

12. Eradication and Recovery Stage

Once the incident is sufficiently contained , the eradication and recovery stage of the IRP can be executed by the Incident Response Coordinator. Prior to any actions being taken in this stage, ensure that evidence will not be compromised by remedial actions and that law enforcement or commercial vendors have been coordinated with.

The objective of this stage is to allow the return of normal operations by eliminating artifacts of the incident (e.g., remove malicious code, re-image infected systems) and mitigating the vulnerabilities or other conditions that were exploited. Before moving to eradication, ensure that all means of persistent access into the network have been accounted for, that the adversary activity is sufficiently contained , and that all evidence has been collected. This is often an iterative process and is possible that eradication and recovery actions can be executed simultaneously.

To validate normal operations have resumed, consider performing an independent test or review of compromise/response-related activity. To help detect related attacks, review cyber threat intelligence (including network situational awareness), and closely monitor the environment for evidence of threat actor activity.

---

13. Post Incident Activity Stage

Following the closure of any incident, the security panel must complete a post-incident review to capture lessons learned, identify improvements, and ensure preventative measures are implemented.

The following checklist should be addressed and documented for every incident:

Policy Gaps – Could an additional policy have prevented the incident?

Policy/Procedure Compliance – Was a policy or procedure not followed, enabling the incident? What steps can be taken to ensure compliance going forward?

Response Effectiveness – Was the incident response appropriate and timely ? How could the response process be improved?

Communication Timeliness – Were all appropriate parties informed in a timely manner ?

Procedure Adequacy – Did the documented incident response procedures cover the full scope of the situation?

Remediation Actions – Have corrective actions been implemented?

Prevention of Recurrence – Have changes been made to prevent a similar or related incident in the future?

Follow-Up Plan – Has a follow-up plan or assessment been established , and are responsibilities and timelines documented?

Risk Management – Was Office of Risk Management notified for assessment of financial/reputational impact and insurance coverage?

---

14. Standards Review

This plan will be reviewed annually by the CIO, CISO, and ITS Security Panel, or sooner if significant changes occur to technology, organizational structure, or applicable regulations.

Effective Date: September 17, 2025
Next Review Date: June 29, 2027
Version: 2.0

Referenced Policies, Standards, and Procedures:

- Data Classification Policy

Appendix A – Security Panel Contact List

Security Panel Contact List		
Christopher Boothman	CIO	870-253-8184
Jacob Weaver	Director of IT Security	870-680-4259
Himaja Balakrishnan	Assistant Vice Chancellor of IT Infrastructure and Operations	870-972-3840
Deanna Warren	Assistant Vice Chancellor/ERP Systems	870-972-3033
Justin Carothers	Senior Director of Academic Technology and Data Analytics	870-680-8332
Vanessa Williams	Budget Director	870-680-4128
San Mirafuentes	Director of Project Management & Communication Services	870-680-4306
Chase Roberson	Senior IT Security Analyst	870-868-1867

Kelsie McDole	Security Operations Center Coordinator	870-680-4273
Law Enforcement Contact List		
University Police Department (UPD): 870-972-2093 (24/7 Dispatch)		
FBI – Jonesboro Resident Agency (Cyber Task Force): 870-932-0700		
Jonesboro Police Department (through UPD coordination): 870-935-5551		

Appendix B – IT Security Incident Report

Date of Report: ___ Prepared By: ___ Incident Date: ___

1. Executive Summary

Brief overview of the incident, severity, and outcome.

2. Incident Overview & Key Timestamps

Identify severity (IRP category), affected assets/data, and critical timestamps (detection, containment, recovery).

3. Initial Indicators

Describe type, initial vector, and IOCs/IOAs.

4. Containment & Mitigation Actions

Document containment steps, approvals, and responsible parties.

5. Evidence Log & Chain of Custody

Record all collected evidence with dates, handlers, and transfers to ensure integrity and a clear chain of custody (if applicable). If UPD/FBI notified, list contact name, agency, and case number obtained.

6. Notifications & Communications

List all internal/external notifications with times and methods.

7. Root Cause Analysis

Summarize underlying vulnerabilities, process gaps, or third-party issues.

8. Timeline of Events

Date	Event Description
ENTER DATE	ENTER TEXT
ENTER DATE	ENTER TEXT
ENTER DATE	ENTER TEXT

9. Lessons Learned

Document what worked, what didn’t, and improvement areas.

10. Recommendations

List technical and procedural remediation items.

11. Review & Approval

Sign-offs by CIO/CISO and Risk Management (if applicable).

4.4 Door Access Control and Security Camera Procurement Procedure

Effective Date: February 26, 2014
Revised Date: May 26, 2026
Responsible Offices: University Police Department (UPD) & Information Technology Services (ITS)
Contact: Randy Martin (UPD) - (870)972-2093 & Heather Boothman (ITS) - (870)972-3933

1. Purpose

This procedure establishes mandatory institutional requirements for the procurement, installation, and integration of door access control systems and security cameras at Arkansas State University. Its purpose is to ensure that all security systems deployed across campus are compatible with enterprise infrastructure, centrally managed, and compliant with university security and safety standards.

---

2. Scope

This procedure applies to all departments, colleges, administrative units, and affiliated entities of Arkansas State University that plan to purchase, install, or upgrade any electronic door access or security camera systems.

It includes all funding sources, procurement methods, and installation types, including purchases construction contracts, or direct requisitions. **Please note, a P-Card should not typically be used for the procurement of security camera systems or installation of electronic door access.**

---

3. Background

Historically, departments independently purchased security and door access control systems that were not compatible with university infrastructure. This practice created fragmented systems, hindered central monitoring, and reduced reliability and effectiveness of campus-wide safety operations.

To address these issues, the Security Task Force and ITS established a unified standard requiring institutional approval and oversight prior to any purchase or deployment of these systems.

4. Standard Requirements

All purchases or installations of security cameras and door access control systems must be approved by the University Police Department (UPD) and Information Technology Services (ITS) before any purchase order or construction contract is initiated.

Approved systems must integrate with:

- The centralized door control infrastructure managed through the Campus Card Center, and
- The central security monitoring systems accessible to UPD for real-time incident response and emergency operations.

All equipment and software must comply with current enterprise technical standards, network security requirements, and access control integration protocols maintained by ITS. Systems that do not meet these standards will not be connected to institutional networks or authorized for monitoring.

---

5. Purchase Procedure

The following procedure outlines the required steps departments must follow to ensure that all door access and security camera purchases are properly reviewed, approved, and integrated into the university's enterprise security and network infrastructure. These steps are designed to maintain system compatibility, uphold security standards, and streamline coordination between ITS, UPD, and the requesting unit.

1. **Pre-Procurement Review**
   Departments must coordinate and submit proposed security camera or door control purchases to ITS and UPD for review prior to procurement. Departments should contact Randy Martin (rmartin@AState.edu) in UPD for security cameras, and for electronic door access control, Heather Boothman in ITS (hboothman@AState.edu). Technical documentation (system specifications, vendor information, and integration details) must accompany the request.
2. **Compatibility Assessment**
   ITS Infrastructure & Networking will review network, power, and system integration compatibility. UPD will review camera placement, field of view, and access configurations for compliance with campus safety objectives.
3. **Approval and Authorization**
   Written approval from both ITS and UPD must be obtained before the procurement process proceeds.
4. **Installation and Verification**
   Upon installation, ITS and UPD will verify system functionality and integration with central management systems.

---

6. Compliance and Enforcement

Failure to obtain approval from ITS and UPD prior to purchase may result in:

- Equipment not being integrated into university systems for monitoring or access control.
- Revocation or cancellation of the purchase order.
- Departmental responsibility for replacement costs to meet compliance standards (if procurement took place without necessary approvals).

Non-compliance will be reported to the respective Vice Chancellor (and/or College Dean) and Procurement Office.

---

7. Student Housing and Residential Use

Students residing in university housing are also subject to institutional policies and housing regulations regarding security devices, monitoring equipment, and recording technologies within residential facilities.

Students should refer to the current Student Handbook and consult with University Housing and/or Student Affairs regarding any questions related to permitted devices, privacy expectations, or residential policies.

Recording and monitoring devices, including but not limited to Ring cameras, doorbell cameras, internal surveillance cameras, or similar recording devices, are not permitted within university housing facilities unless expressly authorized in writing by the university for approved institutional purposes.

The university reserves the right to require removal of unauthorized devices that violate institutional policy, student privacy expectations, housing regulations, or applicable safety and security standards.

---

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 6, 2025
Next Review Date: October 6, 2026
Version: 2.0

Version	Date	Description	Author
1.0	Feb 26, 2014	Original directive/standard established by Security Task Force.	UPD / ITS

2.0	Oct 4, 2025	Reformatted under ITS Standards and Procedures framework in preparation for new university website; modernized language.	UPD / ITS
3.0	May 26, 2026	Added section 7 for Student Housing and Residential Use	UPD / ITS

4.5 ITS Service Commitment & Support Expectations

Service Commitment & Response Expectations

Our Commitment

Information Technology Services (ITS) is committed to providing reliable, responsive, and professional technology support for the Arkansas State University community. Our goal is to ensure that technology issues and service requests are acknowledged promptly, communicated clearly, and resolved as efficiently as possible.

Support Hours
ITS provides support during normal university business hours:
Monday through Friday 8:00 AM to 5:00 PM
Critical technology outages that significantly impact university operations may receive support outside of normal business hours.

What You Can Expect
When you contact ITS, you can expect:

- A timely acknowledgment and initial response regarding your request.
- Clear communication regarding the status of your issue.
- Regular updates when resolution requires additional time.
- Professional and courteous service.
- Prioritization of issues based on their impact to university operations.

Please note that an initial response confirms your request has been received and is being reviewed. It does not necessarily mean the issue has been resolved.

Response Time Expectations

Request Type	Expected Initial Response Time-frame
Email Outreach	Within 0-1 business days
Voicemail Outreach	Within 0-1 business days
Critical Issues	Within 0-30 minutes
High-Priority Issues	Within 0-4 business hours

Standard Support Requests	Within 0-1 business days
Routine Support Requests	Within 0-2 business days

These time-frames represent our goal for acknowledging your request and beginning the support process.

Service Priorities

ITS prioritizes requests according to their impact on university operations. This prioritization helps to ensure requests are handled in an efficient and timely manner while minimizing campus disruption.

Critical Issues

Critical Issues
Examples:

- Campus-wide network outages
- Major system outages
- Significant security incidents

Target Response: Within 15–30 minutes . **Status Updates:** At least hourly until service is restored or stabilized.

High-Priority Issues

High-Priority Issues
Examples:

- Department-wide technology disruptions
- Major service degradation affecting multiple users

Target Response: Within 4 business hours **Target Resolution:** Typically within 1 business day.

Standard Support Requests

Standard Support Requests
Examples:

- Individual account access problems
- Email issues
- General technical support requests

Target Response: Within 1 business day **Target Resolution:** Typically within 3 business days.

Routine Support Requests

Routine Support Requests
Examples:

- Software installations
- Hardware upgrades
- Standard service requests

Target Response: Within 2 business days **Target Resolution:** Typically within 5 business days.

Communication During Resolution
If additional time is needed to resolve your issue, ITS will provide updates appropriate to the priority and complexity of the request. You may be contacted for additional information that is needed to complete the work.

Peak Periods and University Closures

During periods of exceptionally high demand, such as the beginning of academic terms, response and resolution times may be longer than normal. ITS will continue to acknowledge requests as quickly as possible and communicate any significant delays.

How to Receive the Fastest Support

To help us assist you efficiently:

- Submit a service ticket whenever possible.
  - You can submit tickets at: Support Portal
- Provide detailed information about the issue when requesting support.
- Include screenshots or error messages when possible to speed up troubleshooting.
- Respond promptly if we request additional information.

> Unsure of how best to convey your issue? No worries! You can connect with our Help Desk staff using one of the following methods:

Contact IT Help Desk

Phone: 870-972-3933
Email: itshelpdesk@astate.edu
Office Hours: M-F 8am-5pm
After Hours Service is available via Phone

Stop By The IT Support Services Office

First Floor of the Dean B. Ellis Library Room 149
Office Hours: M-F 8am-5pm

> Following these guidelines help to ensure your request is routed to the appropriate support team and tracked through resolution.