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).

Revision #24
Created 2025-10-19 15:40:30 UTC by Christopher Boothman
Updated 2026-10-27 19:56:19 UTC by Jacob Weaver