

Arkansas State University – Information Technology Services

IT Security Incident Response Plan

- 1) The person who discovers the incident will call the ITS Security Panel (See Appendix A for contact information) or email (security@astate.edu) or contact the ITS front desk at 870-972-3033 or after normal business hours, call 870-253-8184.
- 2) The IT Security Panel member who receives the call (or discovered the incident) will notify the Security Panel and appropriate staff members using both email and phone messages while initiating steps to isolate and neutralize the threat. The staff member will log the information received on the attached Incident Identification Form.
- 3) Contacted members of the panel will meet or discuss the situation over the telephone and evaluate current status and assess the incident and additional response requirements.
 - a) Is the incident still in progress? If yes, take immediate action to disconnect or discontinue the incident.
 - b) What data or property is threatened/has been compromised and how critical is it?
 - c) What is the impact if the attack should/has succeed(ed)? Minimal, serious, or critical?
 - d) What system or systems are targeted, where are they located physically and on the network?
- 4) The incident will be categorized into the highest applicable level of one of the following categories:
 - a) Category one - A threat to public safety or life.
 - b) Category two - A threat to sensitive data
 - c) Category three - A threat to computer systems
 - d) Category four - A disruption of services
- 5) In the event of breach of PII, University Legal Counsel will be notified for opinion and recommendations on required notification protocol, etc.
- 6) Do non-Panel members (UPD, Executive Council, University Communications Director) need to be notified and briefed on the incident?
UPD: 870-972-2093
Jonesboro PD: 870-935-5551
FBI: 870-932-0700
- 7) ITS staff members will follow the appropriate procedure based upon the assessment and nature of the incident. See attached Incident Response Procedures/Contact list.
- 8) Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:

- a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence following chain of custody requirements with UPD.
 - b) Make users change passwords if passwords may have been sniffed.
 - c) Be sure the system has been hardened by turning off or uninstalling unused services.
 - d) Be sure the system is fully patched.
 - e) Be sure real time virus protection and intrusion detection is running.
 - f) Be sure the system is logging the correct events and to the proper level.
- 9) Authorized Team members will use forensic techniques, including reviewing system logs, intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.
- 10) Campus wide procedure changes will be presented to Executive Council for approval; departmental changes will be implemented upon CIO approval.
- 11) Documentation—the following shall be documented and filed with the Security Coordinator: (see Incident Identification form)
- a) How the incident was discovered.
 - b) The category of the incident.
 - c) How the incident occurred, whether through email, firewall, etc.
 - d) Where the attack came from, such as IP addresses and other related information about the attacker.
 - e) What was the response.
 - f) Whether the response was effective.
- 12) Evidence Preservation—make copies of logs, email, and other communication will be maintained as evidence as long as necessary to complete investigation, prosecution and beyond in case of an appeal.
- 13) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
- 14) Review response and update procedures using the attached Incident Response Procedure Contacts list.
- 15) Determine the type of follow-up plan/announcement that is required, frequency and timeline. Document the follow-up plan and continue to log status for the duration of timeline.
- 16) Complete the Incident Post Review Checklist and file with Security Coordinator for each incident.

Roles, Responsibilities, and Authority Overview

1. Chief Information Officer (CIO)

- **Responsibilities:**
 - Oversees the entire IT department and ensures alignment with institutional goals.
 - Approves and enforces incident response policies and procedures.
 - Provides direction during security incidents and authorizes major actions such as system shutdowns or isolations.
- **Authority:**
 - Has the final authority on IT decisions impacting critical systems and infrastructure.
 - Collaborates with the IT Security Department and executive leadership to guide incident response efforts.

2. IT Security Department

- **Responsibilities:**
 - Serves as the central team for managing IT security incidents.
 - Coordinates incident detection, investigation, and response efforts.
 - Provides technical expertise to isolate threats, neutralize attacks, and restore services.
 - Ensures documentation of all incidents and adherence to legal and procedural guidelines.
 - May liaise, as needed, with the ITS Security Panel, consisting of representatives from different units within ITS, including Networking, Systems, and Infrastructure.
- **Authority:**
 - Authorized to implement immediate actions to contain and mitigate security incidents.
 - Escalates incidents to executive leadership, legal counsel, or law enforcement when necessary.
 - Can recommend changes in policy and procedure based on incident reviews.

3. Executive Leadership (Chancellor's Cabinet)

- **Responsibilities:**
 - Provides institutional leadership and decision-making in major incidents that impact university operations.
 - Reviews and approves significant changes to security policies and recovery plans proposed by the IT department.
 - Authorizes the allocation of resources (e.g., funding, personnel) required to manage incidents.
- **Authority:**
 - Final authority on decisions involving significant risk or operational disruption to the university.
 - Can direct communications and public relations strategies related to major incidents.

4. General Counsel (Legal)

- **Responsibilities:**
 - Advises the university on legal matters related to data breaches, privacy laws, and regulatory compliance.
 - Provides guidance on required notifications (such as breach notifications to affected

- individuals or regulatory bodies).
- Reviews legal risks associated with IT incidents and guides the institution on potential litigation or regulatory implications.
- **Authority:**
 - Authorized to determine the legal requirements for handling breaches, including communication with law enforcement or third-party investigators.
 - Can direct the institution's legal response in coordination with the IT Security Panel and Executive Leadership.

5. University Communications/Marketing

- **Responsibilities:**
 - Manages internal and external communication strategies during and after IT security incidents.
 - Ensures timely and accurate dissemination of information to stakeholders, including students, faculty, and the public.
 - Works with Executive Leadership to craft public statements that maintain trust and transparency while safeguarding sensitive information.
- **Authority:**
 - Authorized to coordinate media responses and handle inquiries from the public and press.
 - Collaborates with the IT Security Panel and Executive Leadership to ensure alignment on messaging and public relations strategy.

Incident Post Review Checklist

- a) Could an additional policy have prevented the intrusion?
- b) Was a procedure or policy not followed which allowed the intrusion? What could be changed to ensure that the procedure or policy is followed in the future?
- c) Was the incident response appropriate? How could it be improved?
- d) Was every appropriate party informed in a timely manner?
- e) Were the incident-response procedures detailed and did they cover the entire situation?
- f) Have changes been made to prevent a recurrence? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
- g) Have changes been made to prevent a new and similar infection?
- h) Has a follow-up plan/assessment been established?

Appendix A

Security Panel Contact List

Chris Boothman	870-253-8184
Jennifer Harrell	870-253-9417
Patrick Jeffrey	870-680-2110
Senior Security Analyst	<Insert Cell>
Chase Roberson	870-514-9553

Arkansas State University – Information Technology Services IT Security Incident Identification

Date _____ Part 1 of 4

General Information

Incident Detector Information

Name: _____ Date & Time: _____

Title: _____ Cell#: _____

Phone: _____ Location of incident: _____

Email: _____

Incident Summary

Type of Incident Detected:

- Denial of Service
- Unauthorized Use
- Probe
- Hoax
- Malicious Code
- Unauthorized Access
- Other: _____

Incident Location:

Site: _____ Site Point of Contact (POC): _____

POC phone: _____ POC email: _____

How was the incident detected: _____

Additional Information: _____

a) Is the incident still in progress? _____

b) What data or property was threatened/compromised _____

c) Describe impact of the attack - Minimal, serious, or critical? _____

d) What system(s) were targeted? _____

Incident category:

•Category one

•Category two

•Category three

•Category four

Is mandatory notification required? Y/N attach copy of communication piece or other detail

Were non-Panel members notified and briefed on the incident?

•UPD

•Executive Council

•University Communications

•Jonesboro PD:

•FBI

•Other:_____

Check the following to indicate complete or explain below:

_____ Re-install the affected system(s) from scratch and restore data from backups if necessary.

_____ Preserve evidence following chain of custody requirements with UPD.

_____ Make users change passwords if passwords may have been sniffed.

_____ Be sure the system has been hardened by turning off or uninstalling unused services.

_____ Be sure the system is fully patched.

_____ Be sure real time virus protection and intrusion detection is running.

_____ Be sure the system is logging the correct events and to the proper level.

Describe forensic techniques and findings _____

Describe or attach recommended procedural changes _____

Describe the incident, how it was discovered and the response?

Origin of attack? IP addresses and/or other related information

Evidence Preservation:

Damage and cost:

Procedure updates:

Describe follow-up plan/announcement frequency and timeline. Document the follow-up plan and continue to log status for the duration of timeline.
