CYBERSECURITY POLICIES AND PROCEDURES

TABLE OF CONTENTS

INTRODUCTION

The University of Arkansas at Pine Bluff shall provide timely and appropriate notice to affected individuals when there is reasonable belief that a security breach has occurred. A breach in security is defined as an unauthorized acquisition of private and confidential information, typically maintained in an electronic format by the University.

SCOPE

Attacks on University IT resources are infractions of the **APPROPRIATE/ACCEPTABLE USE POLICY** constituting misuse, vandalism, or other criminal behavior. Reporting information security breaches occurring on University systems and/or on University networks to appropriate authorities is a requirement of all persons affiliated with the University in any capacity, including staff, students, faculty, contractors, visitors, and alumni.

DEFINITIONS

Private Information

If the information acquired includes a name (first and last name or first initial and last name) in combination with any of the following, and the information was not in an encrypted format, a public notification may be warranted:

a. Social security number
b. Driver's license Number
c. Bank Account, Credit, or Debit Card Account number with security, access, PIN, or password that would permit access to the account
d. UAPB network password

Personal information that is publicly and lawfully available to the general public, such as address, phone number, and email address are not considered private information for the purposes of this policy.

Highly Sensitive Information

If the information acquired is of a very sensitive, private, confidential, or proprietary nature, the security breach will be investigated and University officials, including the Chancellor and Vice Chancellors, in consultation with the UA System General Counsel, will determine if a public notification is warranted. Examples of highly sensitive information include but are not limited to:

a. Name, Address, with Date of Birth
b. Records protected by FERPA, HIPAA, GLBA, or other applicable federal laws and regulations
c. Confidential research data or results prior to publication
d. Information subject to contractual confidentiality provisions
e. Security codes, combinations, or passwords

POLICIES AND PROCEDURES

Under Board Policy 285.1, University information should be protected from unauthorized access. Campuses and other units shall classify and protect their information in accordance with its value, sensitivity to disclosure, consequences of loss or compromise, and any applicable statutory or regulatory requirements, including the standards and guidelines set by the State Cyber Security Office. Appropriate information security practices shall be undertaken pursuant to a comprehensive security program, which shall include a risk- based framework for identifying and managing threats similar to the framework developed by the National Institute of Standards and Technology in Framework for Improving Critical Infrastructure Cybersecurity.

- The identification of appropriate personnel to lead information-security initiatives and programs on an ongoing basis, including (a) the designation of a technical expert charged with having primary responsibility for information-security matters for the campus or unit and (b) members of a committee to assist with devising policies, critically reviewing operating procedures, evaluating response plans, and similar matters. Input should be received from a range of stakeholders and not just information-technology experts. Administrative units and departments that store highly confidential research data, trade secrets, or personally identifiable information (such as student records, financial information, employee information, and health information) should be involved in the formation and administration of policies pertaining to information security.

- Each campus stakeholder shall ensure that no technology resources across the University are used to express a personal political opinion to an elected official unless the opinion is within the scope of the employee's regular job duties or the opinion is requested by an elected official or public entity; to engage in lobbying an elected official on a personal opinion if the employee is not a registered lobbyist for the campus; to engage in illegal activities or activities otherwise prohibited by federal law or state law; or to intentionally override or avoid the security and system integrity procedures of the campus. Additionally, any political communication must be consistent with Board of Trustees Policy 465.1 and UA System Policy

465.1.

TRAINING

All campus stakeholders will receive comprehensive training annually on the campus's technology resources policy, appropriate use of University-owed equipment and user-owned ("bring your own") devices, maintaining the confidentiality of passwords, understanding the unsecured nature of emails, protecting laptop computers and mobile devices against theft, encrypting removable media and sensitive data that is transmitted on unsecured networks, giving prompt notice of lost devices, hiring and separation procedures, and the latest efforts to defraud employees and students with phishing scams, ransomware, and similar schemes.

ENFORCEMENT

Failure to comply with this Policy puts the University of Arkansas at Pine Bluff, its component institutions, and its information and information technology resources at risk and may result in disciplinary action. Violations of this policy will result in disciplinary action, up to and including termination of employment.

INCIDENT RESPONSE STATEMENT

Suspected or confirmed information security breaches must be reported to University authorities. This includes unauthorized access to UAPB owned technology such as the LAN (local area network), servers, software applications, and other University owned devices. It also includes unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the University of Arkansas at Pine Bluff.

The Vice Chancellor for Finance and Administration will investigate the report, and if a security breach of private and/or highly sensitive information may have occurred, he/she will inform the University Chancellor and/or law enforcement, as appropriate.

In the event that a public notification of the security breach may be warranted, the Vice Chancellor for Finance and Administration will consult with the University Chancellor and appropriate Vice Chancellor(s), Provost, and General Counsel to develop the response and make the final determination if a public notification of the event is warranted.

GENERAL PROCEDURES

The entity responsible for support of the system or network under attack is expected to:

1. Report the attack to their Supervisor and to the Vice Chancellor for Finance and Administration

2. Contact the Director of Technical Services to assess the situation. Technical Services will provide the following:

Analysis:

- Is it a false positive? Review the logs for vulnerability tests or other abnormalities. What systems have been attacked? What stage of the attack? What is theorigin?
- Investigate and look for signs of suspicious activity and data breaches using the following: Firewall and firewall logs; Individual security and audit logs of servers, systems, and Active Directory; Network activity using various networkingtools
- Contact the network provider (AREON) forassistance
- Collect the relevant information:
  - ✓ Date of breach (suspected orknown)
  - ✓ Impact of breach (# of records)
  - ✓ Method of breach (hack, accidental discourse,etc.1.)
  - ✓ Email and phone details
  - ✓ Remediation Status (in progress, completed, and include details)
  - ✓ Next steps (as needed)

Containment:

- Document, block, and/or prevent escalation of the attack, if possible, follow instructions communicated from the Chancellor or the Vice Chancellor for Finance and Administration in subsequent investigation of the incident and preservation ofevidence.
- Implement recommendations from the Chancellor or Vice Chancellor for Finance and Administration. Repair the resulting damage to the system

Communication:

- Follow instructions communicated from the Chancellor or the Vice Chancellor for Finance and Administration in subsequent investigation of the incident and preservation of evidence. Implement recommendations from the Chancellor or Vice Chancellor for Finance and Administration
- Alert everyone on the Incident Response Team including IT, HR, andLegal
- Determine if law enforcement/FBI should be contacted in conjunction with experts in cybersecurity.
- Consideration should be given as to how soon should you alert thepublic.
- The laws vary by state in the US. In the EU, the GDPR says within 72hours.

Eradication:

- Scan all systems for malware.
- Isolate and disable all accounts and components that have beencompromised.
- Remove access to systems by suspect employee logins.
- Change passwords, apply patches, and reconfigure firewalls.
- Repair the resultant damage to the system, if possible.

Recovery:

Prioritize what systems are most critical to resume functionality.

Post-event analysis:

- Record the dwell time (time from data breach to recovery)
- Determine if changes to policies, procedures, or equipment are needed.
- The effectiveness of the incident response plan. Also, test the revised plan using simulated attack.
- Provide cyber awareness training to all employees.

INTERNAL NOTIFICATION

The Chief Information Officer will report serious computer security breaches to the Vice Chancellor for Finance and Administration in a timely manner (no longer than one workday). The Vice Chancellor for Finance and Administration will consult with one or more Vice Chancellors, as appropriate, and decide if the Technical Services Team must be convened to determine a response strategy, or if an alternate group is appropriate for the response. This determination may be made prior to completion of the investigation of the security breach. The Vice Chancellor for Finance and Administration will report the incident to the Chancellor and the UA System General Counsel when, based on preliminary investigation, criminal activity has taken place and/or when the incident originated from a University computer or network.

DETERMINATION OF EXTERNAL NOTIFICATION

To determine if unencrypted private or highly sensitive information has been acquired, or is reasonably believed to have been acquired by an unauthorized person, the following will be considered:

- Physical possession (lost or stolen device?)
- Credible evidence the information was copied/removed
- Length of time between intrusion and detection
- Purpose of the intrusion was acquisition ofinformation
- Credible evidence the information was in a useable format
- Ability to reach the affected individuals
- Applicable University policy, and/or local, state, or federal laws

EXTERNAL NOTIFICATION

If it is determined that an external notification to the affected individuals is warranted, the following procedures will apply:

1. Written notice will be provided to the affected individuals using U.S. Mail, unless the cost is

excessive or insufficient contact information exists. The letter will be developed by the department responsible for the system experiencing the breach and approved by University Relations and approved by the Chancellor. The excessiveness of cost consideration will be the decision of the Chancellor or the UA System General Counsel.

2. If written notice to the affected individuals is not feasible, the following methods will be considered for providing notice:

a. Personal e-mail notices (provided addresses are available), developed by the department responsible for the system experiencing the breach, and approved by the Vice Chancellor for Finance and Administration and other administrators, as appropriate.
b. A press release to media, to be written by University Relations and approved by the Chancellor and other administrators as appropriate.
c. An informational web site developed and hosted by the department responsible for the system experiencing the breach, and approved by the Chancellor, University Public Relations, and others as appropriate, with a conspicuous link on the University public website home page.

3. All expenses associated with external notification will be the responsibility of the department responsible for the system that experienced the security breach.

REFERENCES AND RELATED DOCUMENTS

Researched on the internet and reviewed various Universities' policies online.

POLICY DOCUMENT INFORMATION

Continuous improvement. The content of this document subject to regular review based on input from UAPB Technical Services staff and the campus community. Suggestions for improvement should be directed to the Director of Technical Services.

UAPB Technical Services Incident Report Form
Date and time:
Incident Impact
Impacted services (select one or more): **LAN Internet Access ☐**
WIFI Internet Access ☐
Mitel Phone System ☐
Applications (e.g., Ellucian, Blackboard, WebAdvisor, etc.) ☐
Other ☐
Impact parameters (fill in as appropriate): **Number of users affected per service:_____Incident Duration: _____** **Incident response and recovery actions:** **Issue resolved: Yes☐ No☐**

Root Cause

Root Cause Category:	Initial Cause:	Subsequent Cause:
Human Errors☐	Cable Cut☐	
System Failures☐	Cable Theft☐	
Malicious Actions☐	Flood☐ Storm	
Natural Events☐	☐ Power☐	
Third Party Failure	Power Surges☐	
☐	Physical Attack☐	
	Cyber Attack☐	
	Maintenance☐	
	Overload☐	
	Hardware Failure☐	
	Software Bug☐	
	No Information☐	
	Other☐ _____	

Assets Affected by Initial Cause:

Base stations and controllers☐ **Switches**☐ **Core Network**☐ **Backup Power Supply** ☐

Power supply system☐ **Faculty/Staff**☐ **Students**☐

Other☐ _____