CYBERSECURITY

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*. A comprehensive security program includes, but is not limited to, the following elements:

1. 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.

2. A focus on individual actions and accountability, including initiatives to train employees 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 unsecure nature of emails, protecting laptop computers and mobile devices against theft, encrypting removable media and sensitive data that is transmitted on unsecure 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.

3. An inventory and classification of information in accordance with industry standards and applicable legal requirements.

4. Threat analyses to determine threats to the organization and its data, including cyberattacks and natural disasters; risk assessments to determine the likelihood that a threat could occur and its potential impact; and incident response planning.

5. A program of ascertaining industry best practices and applying them to matters such as backing up data, recovery, encryption, firewalls, anti-virus, anti-malware, security patches, retention of log data and other evidence, and intrusion detection in a manner that is reasonable, effective,

and commensurate with the sensitivity of the information and importance of the information-technology resources at issue.

6. A plan for performing periodic tests, exercises, audits, and post-incident analyses with the goal of determining vulnerabilities, practicing responses, assessing readiness, learning from recent developments, and determining the need to revise policies and procedures.

7. Attention to physical and environmental security, including appropriate security barriers and perimeters to prevent unauthorized access.

8. Sensitivity to the need for contractual counterparties to adopt appropriate practices and give necessary assurances regarding the allocation of duties, liabilities, and risks in the event of a cyberattack—including vendors that maintain personally identifiable information in cloud-based platforms.

9. Each campus 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.

10. Each campus shall have a disciplinary procedure for violation of No. 9 above.

The various campuses and other units of the University of Arkansas System are encouraged to collaborate so that a common, system-wide set of policies and standards can be formulated. At the same time, the President recognizes that differences such as the availability of technical personnel, student enrollment, business operations, financial resources, and information-technology environments differ among the various campuses and other units; therefore, local flexibility in tailoring appropriate policies and procedures must remain intact.

September 22, 2023
May 8, 2017