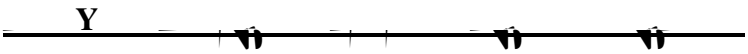

Under Board Policy 285.1, University information should be protected from unauthorized access. Campuses and other units shall classify and protect their information in accordance with its value, sensitivity to disclosure, consequences of loss or compromise, and any applicable statutory or regulatory 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

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