CYBERSECURITY

Information is among the University's most valuable assets. The University often relies on sensitive information to operate effectively and support its central missions of teaching, research, and service. The University consists of research-focused institutions that regularly obtain and store confidential, proprietary data. In addition, the University is frequently required to maintain personally identifiable information that is protected by state and federal law, including education records, health data, and financial information. The security of the University's information, and the technologies and systems that support it, is the responsibility of all employees, vendors, and other stakeholders.

There are numerous persons and organizations who desire to exploit computer systems and acquire intellectual property, personnel information, financial records, and other sensitive information. Cybersecurity threats and information system vulnerabilities are constantly increasing and evolving. The nature of the cybersecurity threats—along with efforts to manage the associated risks—will inevitably grow in complexity.

To efficiently and effectively minimize risks to the confidentiality, integrity, and availability of information, each campus or other unit should employ prudent security policies, technological standards, and safeguards. Sensitive or confidential information that has been created, collected, or distributed by the University should be classified and protected from unauthorized disclosure, access, modification, and destruction. In addition, each campus or other unit should develop an appropriate plan for responding to data breaches and other cyber threats. In furtherance of these objectives, the Board assigns responsibilities as follows:

A. Each chancellor or chief executive is responsible for ensuring that appropriate information security controls are in place for all University information resources and systems. Each chancellor or chief executive should designate an information security committee, which should be tasked with devising policies, providing guidance, assessing the security of network infrastructure, reviewing pertinent operating procedures and response plans, and providing regular reports to the chancellor or chief executive. The person who chairs the committee for the campus or unit should be a person with technical expertise in information security.

B. Each campus or other unit should develop, implement, and maintain a comprehensive information security program that includes a risk-based framework for identifying and managing threats, establishing security standards, responding to incidents, restoring impaired services, and assessing progress toward meeting the program goals.

C. In the event of a material security breach involving the unauthorized acquisition of or access to sensitive information, the information-technology personnel for the campus or unit should promptly contact the appropriate campus administrators and the Office of the General

Counsel. The communication should include a description of the incident, the numbers of individuals impacted, the nature of the information affected, and actions taken to prevent further breaches of security. The Office of the General Counsel shall, in turn, assist campus or unit officials with (i) determining the nature and extent of any notifications to affected persons that may be required by state or federal law and (ii) coordinating any investigations that may need to be conducted by law-enforcement organizations.

March 30, 2017