

CYBERSECURITYI. Purpose

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.

II. Systemwide Information Security Framework

To efficiently and effectively minimize risks to the confidentiality, integrity, and availability of information, the Board requires a systemwide information security governance and information security program that employs prudent security policies, technological standards, and safeguards. Each institution may augment the systemwide information security program with appropriate institution specific supplemental policy and procedure information. 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 furtherance of these objectives, the Board assigns responsibilities as follows:

- A. The System Chief Information Officer (System CIO) will develop and maintain the systemwide information security program and information security governance practices with approval of the President.
- B. The Systemwide Information Security Governance Committee, chaired by the System CIO and consisting of one representative designated by the chancellor or chief executive of each institution, will provide guidance to the System CIO on system information security policies. Each institution's representative will be responsible for ensuring institutional compliance with system information security policies and for coordinating and implementing necessary institutional policies unique to their respective campus, unit or division.

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 affected campus or unit shall promptly notify the appropriate campus administrators, the System CIO, and the Office of the General Counsel. The notification shall include the following:

- i. a description of the incident;
- ii. the number of individuals affected;
- iii. the nature of the information affected; and
- iv. actions taken to prevent further breaches of security.

The Office of the General Counsel shall, in turn, assist campus or unit officials with determining the nature and extent of any notifications to affected persons that may be required by state or federal law and coordinating any investigations that may need to be conducted by law-enforcement organizations.

September 18, 2020 (Revised)
March 30, 2017