3.0075 Security of Data and Related Information Technology Resources

(1) The president of each university shall be responsible for ensuring appropriate and auditable security controls are in place on his/her campus.

(2) Each university shall appoint an information security manager (ISM). This appointment may be combined with other duties/positions and is responsible for administering the information security program/ policies/procedures of his/her respective institution. The name and contact information of the ISM shall be transmitted to the Board of Governors assistant vice chancellor of information technology and security (ITS) each time the appointments given to an individual.

(3) Each university shall develop and annually review and update an information security plan. Each plan may be customized to meet the specific conditions at each university but shall be based upon best practices acquired from recognized national industry standards published by authoritative groups such as: National Institute of Standards (NIST), Information Systems Audit and Control Association (ISACA), International Organization of Standards (ISO), Center for Internet Security (CIS), or other nationally recognized information security organizations.

(4) Each information security plan must address the following:
   (a) The creation of an information security risk management program which includes Risk/Self-Assessment components.
   (b) Compliance with applicable federal and state laws and regulations-as well as contractual obligations-related to privacy and security of data held by the institution.
   (c) Clarifying roles and responsibilities for safeguarding and use of sensitive/ confidential data.
   (d) Creation and maintenance of an inventory of stores of sensitive/ confidential information and who has access to such information.
   (e) Policies and procedures regarding access control and transmission of sensitive/confidential data with an emphasis on providing an auditable chain of custody and encryption.
   (f) Distribution of clear and documented procedures for reporting and handling security violations and the consequences for violating security policies and procedures.
   (g) Methods for ensuring that information regarding the applicable laws, regulations, guidelines and policies is distributed and readily available to computer users.
   (h) Processes for verifying adherence to the information security plan associated policies and procedures.

(5) Each university must make its information security plan, IT audits, IT risk assessments and inventories of known stores of confidential data appropriately available to the Board's assistant vice chancellor of ITS upon request. The items listed above (4a-h) represent a minimum standard for data protection and each university is encouraged to go beyond this minimum standard in its pursuit of data security and integrity.

(6) Cyber Threat Management

   (a) Universities shall use a state-approved cyber threat prohibited technologies list. This list shall be a consolidated list originating from threat intelligence sources, including but not limited to the Federal Department of Homeland Security, the Federal Bureau of Investigations, and the Florida Fusion Center.

   (b) Universities must implement the following protection protocol for identified prohibited

technologies:

1. Prevent identified software network traffic over the university's network, including Wi-Fi.
2. Prevent installation of all identified software from university-owned devices.
3. Remove all identified technologies from university-owned devices or infrastructure.
4. Prevent the installation of any identified hardware within the university's infrastructure.

(c) Exceptions

1. Universities may develop policies and procedures for granting exceptions for the use of identified technologies. Those policies and procedures must include the following components:
   a. A requirement that specific criteria be identified and used for evaluating the need for an exception.
   b. A requirement that exceptions be evaluated by the information security risk management program as established in section (4).
   c. A requirement that all exceptions be reviewed and approved by the university's chief information officer or executive officer identified with similar duties.
   d. A requirement that all exceptions be reviewed and approved by the university's information security manager (ISM).
   e. A requirement that compensating security controls be identified and implemented to limit the risk posed by the specified software or hardware.
   f. Exceptions must be reviewed annually using the defined exception process to determine if continuation is warranted.
2. Law-enforcement exceptions may be granted to enable investigations and other law enforcement activities.

(d) This regulation does not prevent a university from acting against a cyber risk not identified on the Cyber Threat Prohibited Technologies list.

Authority: Section 7(d), Art. IX, Fla. Const., History—New 12-06-07; Amended 06- 28-18, 03-29-23