FLORIDA BOARD OF GOVERNORS
NOTICE OF PROPOSED REGULATION AMENDMENT

DATE: April 4, 2018

REGULATION NUMBER AND TITLE: 3.0075, Security of Data and Related Information Technology Resources

SUMMARY: Revisions to this regulation include changing references from Information Resource Management to Information Technology and Security (ITS) to reflect a recent reorganization and requiring information security plans to be based on best practices from recognized national industry standards published by authoritative groups.

FULL TEXT OF THE REGULATION IS INCLUDED WITH THIS NOTICE.

AUTHORITY TO PROPOSE REGULATION(S): Section 7(d), Art. IX, Fla. Const.; BOG Regulation Development Procedure dated March 23, 2006.

THE BOARD OF GOVERNORS' OFFICIAL INITIATING THE PROPOSED REGULATION: Tim Jones, Vice Chancellor, Finance & Administration

COMMENTS REGARDING THE PROPOSED REGULATION SHOULD BE SUBMITTED WITHIN 14 DAYS OF THE DATE OF THIS NOTICE TO THE CONTACT PERSON IDENTIFIED BELOW. The comments must identify the regulation on which you are commenting:

General Counsel, Board of Governors, State University System, 325 W. Gaines Street, Suite 1614, Tallahassee, Florida 32399, (850) 245-0466 (phone), (850) 245-9685 (fax), or generalcounsel@flbog.edu.

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 ~~Director~~ of Information Technology and Security (ITS)~~Resource Management (who acts as the ISM for the BOG)~~ 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 ~~should~~ shall be based upon best practices acquired from ~~resources such~~ recognized national industry standards published by authoritative groups such as: ~~Educause,~~ 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 ~~sources of~~ information security ~~practices and procedures~~ 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 ~~unknown~~ 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 ~~BOG~~ Board's Assistant Vice Chancellor~~Director~~ of ITS~~IRM~~ upon request.

(6) 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.

Authority: Section 7(d), Art. IX, Fla. Const.; History: New 12-06-07; Amended _____.