Date: December 6, 2007

REGULATION TITLES AND NUMBERS: 3.0075 Security of Data and Related Information Technology Resources

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 Director of Information Resource Management (who acts as the ISM for the BOG) each time the appointment is 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 be based on best practices acquired from resources such as: Educause, National Institute of Standards (NIST) Information Systems Audit and Control Association (ISACA) or other recognized sources of information security practices and procedures.

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 known 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 and 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 Director of 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.

Specific Authority: Section 7(d), Article IX, Florida Constitution