5.5	IT Policy - Design, Implementation Operational Management and Assurance/Compliance of the Information Security Program	13-138	2013-10-17

5.5   Design, Implementation Operational Management and Assurance/Compliance of the Information Security Program

To meet the missions of the BOR constituent units of providing affordable higher education the BOR needs to evaluate organizational and operational changes that will maximize the efficiency and effectiveness of its Information Security Program; and

The BOR must assure that all ConnSCU constituent units maintain an Information Security Program ("ISP") that is consistent. It is critical that the BOR implement in a timely manner new logical and technical controls to protect the BOR confidential data and infrastructure from future breaches

The BOR Chief Information Officer shall be responsible for the design, implementation, operations and compliance functions of the Information Security Program for all ConnSCU constituent units.

The college and university Presidents are responsible for assuring that the BOR Information Security Program inclusive of all standards, procedures, and compliance - including managerial, operational and technical controls is followed by their institution; therefore be it

Security, standards, procedures, and compliance - including managerial, operational and technical controls - shall be consistent with the National Institute of Standards (NIST). Further, standards and procedures for protecting information shall be consistent with state and federal laws, including but not limited to FERPA and GLBA, and be it

All senior managers whose staff use personally identifiable information in the carrying out their institutional duties shall ensure that their staff have been provided the appropriate level of data security awareness training and are in ongoing compliance with data security standards and practices.

All costs associated with mitigating security breaches due to a constituent's failure to comply with the BOR Information Security Program shall be the responsibility of the respective BOR constituent.

The BOR Chief Information Officer shall annually provide the Board of Regents a report detailing the security program effectiveness and the risk the BOR is currently accepting. The report will be provided by November 15.