CT BOARD OF REGENTS FOR HIGHER EDUCATION

RESOLUTION

concerning

The Design, Implementation Operational Management and Assurance/Compliance of the Information Security Program for the Board of Regents of Higher Education

October 17, 2013

WHEREAS, The Board of Regents for Higher Education (BOR) for the Connecticut State Colleges and Universities (ConnSCU) recognizes that unauthorized disclosure of certain personal information is prohibited by various state and federal statutes, and

WHEREAS, The Board of Regents (BOR) for the ConnSCU recognizes that the implementation of an Information Security Program is mandated by state and federal statutes, including but not limited to: Connecticut General Statutes Section 36a-701b et seq., Family Educational Rights and Privacy Act (FERPA) 20 USC §1232g , Gramm-Leach-Bliley Act (GLBA) 16 USC §314, e-Discovery, Health Insurance Portability and Accountability Act (HIPPA), and Electronic Communication Privacy ACT (ECPA) 18 USC § 2510, and

WHEREAS, The Board of Regents (BOR) for the Connecticut State Colleges and Universities (ConnSCU) recognizes that information security needs to address availability, confidentiality and integrity of ConnSCU information whether in electronic or paper form.

WHEREAS, 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

WHEREAS, The BOR must assure that all ConnSCU constituent units maintain an Information Security Program (“ISP”) that is consistent, and

WHEREAS, 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; therefore be it

RESOLVED, That 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; therefore be it

RESOLVED, That 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

RESOLVED, That security, standards, procedures, and compliance - including managerial, operational and technical controls - shall be consistent with the National Institute of Standards (NIST), and be it

RESOLVED, That 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

RESOLVED, That 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; and be it further

RESOLVED, That 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; and be it further

RESOLVED, That 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.

A True Copy:

Erin A. Fitzgerald, Secretary of the
CT Board of Regents for Higher Education

ITEM

Resolution concerning leadership, responsibility, design, implementation, operational management and compliance of the Connecticut State Colleges and Universities (ConnSCU) Information Security Program for the Board of Regents for Higher Education (BOR) and its Institutions

BACKGROUND

Information security management is not just a legal obligation. It also reflects the Board of Regent's commitment to the ethical collection, use, sharing, protection, retention, availability and integrity of information. The BOR has experienced information security breaches in the past and wants to ensure that a consistent Information Security Program exist for all constituent units. It is critical that the BOR has consistent policies and understanding surrounding authority, responsibility and accountability for information security oversight, compliance, risk assessment and mitigation. The proposed resolution draws from the common practices and guidance by the National Institute of Standards and Technology (NIST) on the design, implementation, operations and compliance of an Information Security Program.

ANALYSIS

The review current security practices have highlighted potential vulnerability and risks associated with information security at Board of Regents of Higher Education and its institutions. Consistent with best practices, the resolution clearly establishes the roles and authorities of the Board regarding information security matters and provides that the implementation of information security program will be reviewed, updated, or enhanced on an annual basis. The resolution, when fully implemented, will provide for appropriate accountability, responsibility and transparency.

RECOMMENDATION

The Board of Regents approves the following Resolution concerning Leadership, Responsibility, and Ongoing Operational Management of the Information Security Program for the Board of Regents for Higher Education and its Institutions.

9/19/13 – Information Technology
10/17/13 – Board of Regents