RESOLUTION

Concerning

The Leadership, Responsibility, and On-going Operational Management of the Information Security Programs for the Board of Regents of Higher Education and its Institutions

June 21, 2012

WHERAS, The Board of Regents (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, including but not limited to: Connecticut General Statutes Section 36a-701b et seq., Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPPA), and Electronic Communication Privacy ACT (ECPA), and

WHERAS, The BOR must assure that all institutions and the Board office maintain an Information Security Program ("ISP"); and

WHERAS, The increasing use of internet resources, mobile computing and storage devices along with the increasing sophistication and volume of malware has significantly increased the risk of confidential data being misplaced, exposed to unauthorized users, or breached by hackers; and

WHERAS, The substantial monetary loss and reputation damage associated with security breaches require that the BOR looks for organizational and operational changes that will maximize the efficiency and effectiveness of its ISP; therefore be it

RESOLVED, That the college and university Presidents are responsible for the implementation and maintenance of an ISP at their institution; and be it further

RESOLVED, That the senior IT leaders of colleges and universities shall implement the recognized security controls practiced in the industry; apprise the Presidents of all unmitigated risks in privacy and security at their respective institutions; and be it further

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 the BOR Chief Information Officer shall oversee all investigations and responses related to unauthorized access and/or disclosure of sensitive information as well as all computer security incidents to minimize risk to BOR and its institutions; and be it further

RESOLVED, That all costs associated with mitigating security breaches shall be the responsibility of the institution or office that was responsible for on-going operational management of security controls; and be it further

RESOLVED, That each institution shall annually provide the Board of Regents a report detailing the security controls implemented at their locations with the first report be completed by September 1, 2012. The report shall describe controls in firewall management, network intrusion detection and mitigation, patch management, virus detection and mitigation, incident response management, data stewardship, training, and risk management.