

South Carolina Higher Education Tuition Grants Commission

115 Atrium Way, Suite 102; Columbia, SC 29223 Phone: (803) 896-1120 Fax: (803) 896-1126

AGENCY SECURITY MEASURES UPDATE

Prepared for Commission Meeting

June 14, 2016

The agency has completed the creation of required Information Security Policies and Procedures Manuals ahead of the State's July 1, 2016 deadline. The Policies document was finalized and approved by the agency director, as required, on December 18, 2015. The final step of the process is for the Commission to review and give final approval to the Procedures document, which is used to show the agency's compliance efforts concerning the thirteen information security policies mandated by the State.

Prior to today's Commission Meeting, all Commission Members were provided with a copy of the full document for review. The following is a summary of the objectives of each section of the manual:

Section I – Information Security Governance

- Discusses responsibilities of agency management to appoint the appropriate personnel, resources, and internal controls in order to support the agency's implementation of and compliance with InfoSec policies; Oversight authority to agency management.

Section II – Asset Management

- Discusses parameters for the compliant inventory of IT-related assets to include information identifying business owner, data classification, asset location, and security impact analysis of all agency IT assets (i.e., computers, router, switch, flash drives, wireless access point, etc.).

Section III – Data Protection and Privacy

- Discusses agency's responsibility to correctly classify data and to place security controls on any confidential, restricted, or sensitive information housed by the agency; Discusses agency's responsibility to sanitize any media prior to disposal; Discusses agency's adoption of its Privacy Impact Assessment (privacy statement on website).

Section IV – Access Control

- Discusses Separation of Duties requirements, role-based access control to agency personnel, system password requirements, session locks, and other tools and processes available to ensure the approved system users have access to the correct information based on their job responsibilities.

Section V – IS Acquisitions, Development, and Maintenance

- Discusses security requirements for change management procedures for agency systems, including testing and deployment environments, and maintenance of a secure baseline configuration.

Section VI – Threat and Vulnerability Management

- Discusses the agency's partnership with the Department of Technology Operations as related to monitoring of the information system, penetration testing schedule, patch management processes, and incident management and response.

Section VII – Business Continuity Management

- Discusses the requirement for the agency to have a Disaster Recovery Plan in the event information systems are disabled or destroyed; this plan includes backup of agency data (including a secondary, off-site backup location), emergency telecommunications services options, and options for alternative remote working environments in order to continue critical agency operations during a disaster; Establishes agency's Recovery Point Objective and Recovery Time Objective, based on a criticality assessment previously performed with the Division of Information Security.

Section VIII – IT Risk Strategy

- Discusses allowable data sharing agreements with third parties and other agencies; this includes the completion of Security Agreements and Memoranda of Understanding, as required.

Section IX – Mobile Security

- Discusses acceptable mobile device usage and limited connectivity options via the agency's wireless access point; at this time, the agency does not issue any mobile computing or telephone devices to any agency personnel, and personal mobile devices are limited to internet connectivity only. The agency does not allow access to its servers, files, or systems via mobile devices, with the exception of a laptop owned by the IT Contractor who works remotely and connects to a limited-access test data environment through a two-factor authentication and VPN process.

Section X – Human Resources and Security Awareness

- Discusses annual Information Security/Cyber-Security training requirements and monitoring of training completion for all agency personnel utilizing the SANS Securing the Human training platform.

Section XI – Physical and Environmental Security

- Discusses access controls procedures to the agency's physical equipment, property, and files, including access limitations (locked doors, building security features), visitors log requirements, and emergency shutoff to agency's internal datacenter; this procedure also outlines the responsibilities of the Department of Technology Operations in the area of protecting the agency's server location on their premises (i.e., temperature and humidity control, fire protection, water protection, and limitation of access).

Section XII – Risk Management

- Discusses the authorization of agency management to review and determine whether or not certain risks can be accepted and to develop corrective action plans, as necessary, to correct any deficiencies discovered during security assessments.

Section XIII – IT Compliance

- Discusses the agency's obligation to perform periodic compliance reviews/audits as related to the Information Security policies and procedures; these reviews are completed with assistance from subject-matter experts available through the State's Division of Information Security, Department of Technology, and Enterprise Privacy Office.