STATE BOARD FOR TECHNICAL AND COMPREHENSIVE EDUCATION

STATEMENT OF POLICY

POLICY NUMBER: **4-4-105**

PAGE: **1 of 6**

POLICY TITLE: **INFORMATION SECURITY**

LEGAL AUTHORITY: **Section 59-53-57 of the 1976 Code of Laws of South Carolina, As Amended**

DIVISION OF RESPONSIBILITY: **INFORMATION TECHNOLOGY**

DATE APPROVED BY BOARD: **September 27, 2011**

DATE OF LAST REVISION: **October 3, 2017**

CHAIRMAN **EXECUTIVE DIRECTOR**

The State Board for Technical and Comprehensive Education (State Board) is committed to protecting the confidentiality, integrity, and availability of its information assets. Information assets are defined as all information, regardless of the form or format, which is created, acquired

or used within the South Carolina Technical College System (System). This policy applies to information recorded on any media or device, including those owned by the System, college, or individual.

The State Board is committed to ensuring an environment that will assist in protecting all members of the System from information security threats that could compromise privacy, productivity or reputation. This policy also applies to all individuals who access computer networks or information assets of the System.

All colleges and the system office shall ensure compliance with all applicable Federal, State and local laws and regulations, and should develop more specific procedures that follow Information Security best practices to appropriately address the protection of and access to data and Information Technology assets.

The following sections provide a broad framework for developing the South Carolina Technical College System (SCTCS) information security plan. An effective information security plan improves all the colleges' and the system office's security posture and aligns information security with their mission, goals, and objectives. Implementation of the information security program by all the colleges and the system office must comply with the policy framework established by the state of South Carolina and federal standards, as published in the Policies section of the SC DIS website: http://www.admin.sc.gov/technology/information-security.

1.0 INFORMATION SECURITY PROGRAM

The SCTCS Information Security (InfoSec) Program consists of information security policies, procedures, and other guidance that establish a common information security framework across all colleges and the system office within the South Carolina Technical College System.

All colleges and the system office shall develop and communicate an information security plan that defines security requirements, and the controls in place for meeting those requirements.

2.0 ASSET MANAGEMENT

The purpose of the Asset Management section is to define the basis for developing an inventory of assets and classification of data that support the SCTCS.

All colleges and the system office shall document and maintain inventories of the important assets associated with each information system.

All colleges and the system office shall classify assets into the data classification types in the State of South Carolina Data Classification Schema.

3.0 ACCESS CONTROL

The purpose of Access Control is to establish processes to control access and use of SCTCS information resources, to establish procedures to control and monitor access and use of the network infrastructure, to establish a standardized method to create and maintain verifiable user identifiers, to establish the authentication methods utilized by the SCTCS, and to establish conditions under which emergency access is granted.

All colleges and the system office shall establish formal, documented procedures needed to implement an access control policy and associated access controls.

4.0 DATA PROTECTION AND PRIVACY

The purpose of Data Protection and Privacy is to define the different categories for SCTCS information assets regardless of form, to define the controls that need to be in-place to protect confidential and restricted data, and to set forth policies the college system shall use when information systems or applications gather Personal Identifiable Information (PII) and/or when webpages are available openly to the public.

All colleges and the system office shall categorize data in accordance with applicable federal and State laws and regulations.

All colleges and the system office shall develop a list of approved processes for sanitizing electronic and non-electronic media prior to disposal, release and reuse.

All colleges and the system office shall develop processes for transmitting data.

For Restricted or data protected by Federal or State laws or regulations: SCTCS shall use Federal Information Processing Standards (FIPS)-140 validated technology for encrypting confidential data.

5.0 INFORMATION SYSTEMS ACQUISITIONS, DEVELOPMENT, AND MAINTENANCE

All colleges and the system office shall define change management controls to manage changes to information systems.

All colleges and the system office shall comply with established security standards and state procurement guidelines for critical enterprise information systems or systems under development.

6.0 THREAT AND VULNERABILITY MANAGEMENT

All colleges and the system office shall establish controls and processes to help identify vulnerabilities within the SCTCS technology infrastructure and information system components which could be exploited by attackers to gain unauthorized access, disrupt business operations, and steal or leak sensitive data, and to also establish controls and processes that will provide effective monitoring and response against these threats.

All colleges and the system office shall develop an incident response plan.

7.0 INFORMATION TECHNOLOGY SYSTEMS CONTINUITY MANAGEMENT

The purpose of the Information Technology Systems Continuity Management planning section is to establish procedures and processes to maintain continuity of critical information technology systems during or post an incident.

All colleges and the system office shall develop a Disaster Recovery Plan (DRP) that addresses scope, roles, responsibilities, and coordination among organizational entities for reallocating information systems operations to an alternate location.

8.0 INFORMATION TECHNOLOGY RISK MANAGEMENT

The purpose of the Information Technology Risk Management section is to establish controls to assess the performance of the security program and its components, to identify and assess information security risks, and to take steps to reduce risk to an acceptable level.

All colleges and the system office shall monitor and the adoption of security controls, and associated policies and procedures, and effectiveness of the information security program.

All colleges and the system office shall establish a risk assessment framework based on applicable State and federal laws, regulation, and industry standards (e.g., NIST 800-30).

All colleges and the system office shall establish processes to enforce that third parties comply with information security requirements.

9.0 MOBILE SECURITY

The purpose of the Mobile Security section is to describe the minimum security required for removable media and mobile and portable computing devices used to access State data, including usage restrictions, configuration management, device authentication, and implementation of mandatory security software.

All colleges and the system office shall develop usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile and portable computing devices.

All colleges and the system office shall protect information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures.

10.0 HUMAN RESOURCE AND SECURITY AWARENESS

The purpose of the Human Resource (HR) and Security Awareness section is to define security roles and responsibilities for employees, contractors and third party users, and to define the information security training requirements for SCTCS employees, contractors and third party users.

All colleges and the system office shall establish a Statement of Acceptable Use document governing the use of computers, electronic devices, network services and the Internet.

All colleges and the system office shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.

All colleges and the system office shall adopt policies intended to reduce the ability of the user to access web sites displaying information or material in violation of Article 3 of Chapter 15 of Title 16 from the South Carolina Code of Laws.

All colleges and the system office shall define security roles and responsibilities of employees, contractors and third party users and shall be documented in accordance with the organization's information security procedures.

All colleges and the system office shall impart appropriate awareness training and regular updates in organizational policies and procedures to all employees of the organization as relevant for their job function.

All contractors or third parties will adhere to all security awareness training as outlined in their procurement contract.

11.0 PHYSICAL AND ENVIRONMENTAL SECURITY

All colleges and the system office shall establish controls to prevent unauthorized physical access to SCTCS information assets, and to protect them from damage, interruption, misuse, destruction, environmental factors and/ or theft.