TECHNICAL COLLEGE
OF THE LOWCOUNTRY

POLICY: Information Technology Security
Number: 2.3.2

Responsibility:	Administrative Services (Information Technology Department)
Last Updated:	October 1, 2022
State Policy/Law:	SBTCE Policy 4-4-105

______________________________ ______________________________
Commission Chair President

The Technical College of the Lowcountry 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. This policy applies to information recorded on any media or device, including those owned by the System, College, or individual.

The College is committed to ensuring an environment 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.

The College 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.

Information Security Program

The TCL Information Security (InfoSec) Program consists of information security policies, procedures, and other guidance that establish a common information security framework across the institution.

The Technical College of the Lowcountry shall develop and communicate an information security plan that defines security requirements, and the controls in place for meeting those requirements.

Asset Management

The Asset Management section aims to define the basis for developing an inventory of assets and the classification of data that supports TCL.

The college shall document and maintain inventories of the important assets associated with each information system.

The college shall classify assets into the data classification types in the State of South Carolina Data Classification Schema.

Access Control

The purpose of Access Control is to establish processes to control access and use of TCL 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 TCL, and to establish conditions under which emergency access is granted.

The Technical College of the Lowcountry shall establish formal, documented procedures needed to implement an access control policy and associated access controls.

Data Protection and Privacy

The purpose of Data Protection and Privacy is to define the different categories for TCL 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.

The Technical College of the Lowcountry shall categorize data in accordance with applicable federal and State laws and regulations.

The Technical College of the Lowcountry shall develop a list of approved processes for sanitizing electronic and non-electronic media prior to disposal, release, and reuse.

The Technical College of the Lowcountry shall develop processes for transmitting data.

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

Information Systems Acquisitions, Development, and Maintenance

The Technical College of the Lowcountry shall define change management controls to manage changes to information systems.

The Technical College of the Lowcountry shall comply with established security standards and state procurement guidelines for critical enterprise information systems or systems under development.

Threat and Vulnerability Management

The Technical College of the Lowcountry shall establish controls and processes to help identify vulnerabilities within the TCL 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.

The Technical College of the Lowcountry shall develop an incident response plan.

Information Technology Systems Continuity Management

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

The Technical College of the Lowcountry shall develop procedures that address the scope, roles, responsibilities, and coordination among organizational entities for reallocating information systems operations to an alternate location.

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.

The Technical College of the Lowcountry shall monitor the adoption of security controls, associated policies, and procedures, and the effectiveness of the information security program.

The Technical College of the Lowcountry shall establish a risk assessment framework based on applicable State and federal laws, regulations, and industry standards (e.g., NIST 800-30).

The Technical College of the Lowcountry shall establish processes to enforce that third parties comply with information security requirements.

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.

The Technical College of the Lowcountry shall develop usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile and portable computing devices.

The Technical College of the Lowcountry shall protect information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures.

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 TCL employees, contractors, and third-party users.

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

TCL shall require employees, contractors, and third-party users to apply security in accordance with established policies and procedures of the organization.

TCL shall define the security roles and responsibilities of employees, contractors, and third-party users and shall be documented in accordance with the organization’s information security procedures.

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

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

Physical and Environmental Security

The Technical College of the Lowcountry shall establish controls to prevent unauthorized physical access to TCL information assets, and to protect them from damage, interruption, misuse, destruction, environmental factors, and/ or theft.

Procedures:

2.3.2.1 - Systems Security and Authorization
2.3.2.2 - System Backups
2.3.2.3 - Acceptable Use of Information Resources
2.3.2.4 - Incident Response Plan