TECHNICAL COLLEGE
OF THE LOWCOUNTRY

PROCEDURE: Systems Security and Authorization
Number: 2.3.2.1

Responsibility:	Administrative Services (Information Technology Department)
Last Updated:	November 1, 2023
Related Policy:	2.3.2 Information Technology Security

_____

President

Purpose:

The purpose of this procedure is to provide guidelines for security and authorization needed to maintain data processing services to users, while ensuring informational privacy to comply with college policies and applicable federal and state laws.

Procedure:

Chief Information Officer Responsibilities

1. Ensure the physical and data security of computing resources and investigate security breaches.
2. Define user privileges.
3. Instruct all employees in computer security fundamentals and attempt to identify and eliminate practices that expose the College to unnecessary risk.

Access to the IT Data Center

1. The CIO will maintain strict lock combination control and other means of security to preclude unauthorized access to the Data Center. The door combination will be changed regularly.
2. If outside personnel need to enter the Data Center, they must have approval from IT and be accompanied by an IT staff member.
3. Students are not allowed entry to the IT offices. Exceptions are made only for work study students employed by IT. Work study students are allowed in the offices only when an IT staff member is present.

System Controls
Controls include but are not limited to the following:

1. Granting access: IT will establish access for new employees to needed resources upon official notification of the employee's hire. Official notification must come from either the HR department or the new employee's department head.
2. Password policies: The IT department will establish and enforce password complexity and rotation requirements.
3. Remote access via VPN or remote dial-in will be granted only by request and after review and approval by the respective Vice President, Dean, or President.
4. Appropriate file permissions will be applied to control access to shared files.
5. Monitoring user accounts and network traffic to ensure appropriate use: All data and programs on campus computing systems as well as Internet bandwidth provided by the College are the property of the Technical College of the Lowcountry. The College's computer resources are provided to support the education of students and perform the administrative functions of the College. Misuse of these resources can result in disciplinary action. Use of these resources may be inspected at any time upon the request of an employee's supervisor and approval from HR, or in response to an external legal or FOIA request.
6. Employee Termination: Immediately upon termination of an employee, the Personnel Director will notify the IT Department which will then cancel the terminated employee's computer privileges.

Security Breaches

1. The CIO investigates any known breaches, suspected breaches, or attempts to breach computer system security, and initiates appropriate protective actions.
2. If, in an emergency, the CIO is not available, another member of the IT staff may initiate appropriate protective action.
3. In cases that involve students the Associate Vice President for Student Affairs is notified. In cases involving faculty or student affairs staff, the Vice President for Academic Affairs/Student Affairs is notified. In cases involving administrative services staff, the Vice President for Administrative Services is notified.
4. Any disciplinary actions involving security breaches or improper use of computing resources are handled by the appropriate College committee in the cases of students or by the appropriate supervisor in the case of employees. Serious cases will be referred to local law enforcement for prosecution.
5. In an emergency in which clear and present physical danger to College students, personnel, equipment, or information exists, protective measures may be invoked prior to the notification of the relevant senior official. In any such case, immediate follow up with the appropriate senior official(s) will be made.

Academic Computing

1. Students are not allowed access to the administrative systems of the College, except in the case of Work Study students, where such access is a component of their job.

2. Students who illegally access computer files or otherwise abuse computing resources and privileges will be subject to discipline under College guidelines and will be subject, as well, to appropriate civil and criminal action.

Responsibilities of Individual Employees

1. Each individual is accountable for his/her conduct in the use of computing resources. Each computer user must:
    a. Keep access passwords secret.
    b. Log off or lock their workstation when leaving a system unattended.
    c. Immediately report observed violations of any security requirements to the IT Director.
2. Every individual who is authorized to use TCL's computing facilities must adhere to all relevant computing guidelines, including Acceptable Use policies.