TECHNICAL COLLEGE
OF THE LOWCOUNTRY

PROCEDURE: Student Acceptable Use
Number: 2.3.2.5

Responsibility: Administrative Services (Information Technology Department)
Approval Date: August 14, 2024
Related Policy: 2.3.2 Information Technology Security

____
President

Procedure:

Student Responsibilities

1. Students are responsible for complying with TCL policies when using TCL information resources. If requirements or responsibilities are unclear, please seek assistance from the IT department.
2. Students must promptly report harmful events or policy violations involving TCL assets or information on TCL's Center for Information Security at https://www.tcl.edu/tcl-center-for-cybersecurity/. Click on "Report an Incident". Events include, but are not limited to, the following:
   a. Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability of TCL information resources.
   b. Data incident: any potential loss, theft, or compromise of TCL information.
   c. Unauthorized access incident: any potential unauthorized access to a TCL information resource.
   d. Facility security incident: any damage or potentially unauthorized access to a TCL-owned, leased, or managed facility.
   e. Policy violation: any potential violation to this or other TCL policies, standards, or procedures.
3. Students should not purposely engage in activities that may:
   a. harass, threaten, impersonate, or abuse others.
   b. degrade the performance of TCL information resources.
   c. deprive authorized TCL students access to a TCL information resource.
   d. obtain additional resources beyond those allocated.
   e. or circumvent TCL computer security measures.
4. Students should not download, install, or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, TCL students should not run password-cracking programs, packet sniffers, port scanners, or any other non-approved

programs on any TCL information resource.

5. Use of encryption should be managed in a manner that allows designated TCL students to promptly access all data.
6. TCL information resources are provided to facilitate learning and should not be used for personal financial gain.
7. Students are expected to cooperate with incident investigations, including any federal or state investigations.
8. Students are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using TCL information resources.
9. Students should not intentionally access, create, store or transmit material which TCL may deem to be offensive, indecent, or obscene.

Access Management

1. Access to information is based on a "need to know" basis.
2. Students are permitted to use only those network and host addresses issued to them by TCL IT and should not attempt to access any data or programs contained on TCL systems for which they do not have authorization or explicit consent.
3. All remote access connections made to internal TCL networks and/or environments must be made through approved, and TCL-provided, virtual private networks (VPNs).
4. Students should not divulge any access information to anyone not specifically authorized to receive such information, including IT support.
5. Students must not share their personal authentication information, including:
    a. Account passwords,
    b. Personal Identification Numbers (PINs),
    c. Security Tokens (i.e. Smartcard),
    d. Multi-factor authentication information
    e. Access cards and/or keys,
    f. Digital certificates,
    g. Similar information or devices used for identification and authentication purposes.
6. Access cards and/or keys that are no longer required must be returned.
7. Lost or stolen access cards, security tokens, and/or keys must be reported as soon as possible.
8. A service charge may be assessed for access cards, security tokens, and/or keys that are lost, stolen, or are not returned.

Authentication/Passwords

1. All students are required to maintain the confidentiality of personal authentication information.
2. Any group/shared authentication information must be maintained solely among the authorized members of the group.
3. All passwords, including initial and/or temporary passwords, must be constructed, and implemented according to the following TCL rules:
    a. Must meet all requirements including minimum length, complexity, and reuse

    history.
  b. Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.
  c. Must not be the same passwords used for personal purposes.
4. Unique passwords should be used for each system, whenever possible.
5. User account passwords must not be divulged to anyone. TCL support staff and/or contractors should never ask for user account passwords.
6. If the security of a password is in doubt, the password should be changed immediately.
7. Students should not circumvent password entry with application remembering, embedded scripts or hard-coded passwords in client software.
8. Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with TCL, if issued.

Email and Electronic Communication

1. Auto-forwarding electronic messages outside the TCL internal systems is prohibited. Electronic communications should not misrepresent the originator or TCL.
2. Students are responsible for the accounts assigned to them and for the actions taken with their accounts.
3. Accounts must not be shared without prior authorization from TCL IT, with the exception of calendars and related calendaring functions.
4. Any personal use of TCL provided email should not:
    a. Involve solicitation.
    b. Be associated with any political entity
    c. Have the potential to harm the reputation of TCL.
    d. Forward chain emails.
    e. Contain or promote anti-social or unethical behavior.
    f. Violate local, state, federal, or international laws or regulations.
    g. Result in unauthorized disclosure of TCL confidential information.
    h. Or otherwise violate any other TCL policies.
5. Students should only send confidential information using approved secure electronic messaging solutions.
6. Students should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.

Internet

1. The Internet must not be used to communicate TCL confidential or internal information, unless the confidentiality and integrity of the information is ensured, and the identity of the recipient(s) is established.
2. Use of the Internet with TCL networking or computing resources must only be used for learning-related activities. Unapproved activities include, but are not limited to:
    a. Accessing or distributing pornographic or sexually oriented materials
    b. Attempting or making unauthorized entry to any network or computer accessible from the

    c. Internet.
    d. Or otherwise violating any other TCL policies.

3. Access to the Internet from outside the TCL network using a TCL-owned computer must adhere to all the same policies that apply to use from within TCL facilities.

Privacy

1. Information created, sent, received, or stored on TCL information resources are not private and may be accessed by TCL IT employees at any time, under the direction of TCL executive management and/or Human Resources, without knowledge of the user or resource owner.
2. TCL may log, review, and otherwise utilize any information stored on or passing through its information resources systems.

Enforcement

Students found to have violated this policy may be subject to disciplinary action.

Acknowledgement

I have reviewed and understand the contents of the Technical College of the Lowcountry's Student Acceptable Use Policy and will abide by its contents.

______________________________ ______________________________ __________________

Student's Full Printed Name Student's Signature Date