TECHNICAL COLLEGE
OF THE LOWCOUNTRY

PROCEDURE: Acceptable Use of Information Resources
Number: 2.3.2.3

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 establish acceptable practices regarding the use of Technical College of the Lowcountry information resources in order to protect the confidentiality, integrity and availability of information created, collected, and maintained. The procedure applies to any individual, entity, or process that interacts with any TCL information resource.

Procedure:

Personnel Responsibilities

1. Personnel are responsible for complying with TCL policies when using TCL information resources and/or on TCL time. If requirements or responsibilities are unclear, please seek assistance from the IT department.
2. Personnel must promptly report harmful events or policy violations involving TCL assets or information to their manager or a member of the IT department. 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 to 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. Personnel should not purposely engage in activity that may
    a. harass, threaten, impersonate, or abuse others;
    b. degrade the performance of TCL information resources;

   c. deprive authorized TCL personnel access to a TCL information resource;
   d. obtain additional resources beyond those allocated;
   e. or circumvent TCL computer security measures.
4. Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, TCL personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any TCL information resource.
5. All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on TCL time and/or using TCL information resources are the property of TCL.
6. Use of encryption should be managed in a manner that allows designated TCL personnel to promptly access all data.
7. TCL information resources are provided to facilitate college business and should not be used for personal financial gain.
8. Personnel are expected to cooperate with incident investigations, including any federal or state investigations.
9. Personnel 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.
10. Personnel 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. Personnel 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. Personnel should not divulge any access information to anyone not specifically authorized to receive such information, including IT support personnel.
5. Personnel 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 to physical security personnel.
7. Lost or stolen access cards, security tokens, and/or keys must be reported to physical security personnel 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 personnel 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 non-business purposes.
4. Unique passwords should be used for each system, whenever possible.
5. User account passwords must not be divulged to anyone. TCL support personnel 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. Personnel 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.

Clear Desk/Clear Screen

1. Personnel should log off from applications or network services when they are no longer needed.
2. Personnel should log off or lock their workstations and laptops when their workspace is unattended.
3. Confidential or internal information should be removed or placed in a locked drawer or file cabinet when the workstation is unattended and at the end of the workday if physical access to the workspace cannot be secured by other means.
4. Personal items, such as phones, wallets, and keys, should be removed or placed in a locked drawer or file cabinet when the workstation is unattended.
5. File cabinets containing confidential information should be locked when not in use or when unattended.
6. Physical and/or electronic keys used to access confidential information should not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
7. Laptops should be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday if the laptop is not encrypted.
8. Passwords must not be posted on or under a computer or in any other physically accessible location.

9. Copies of documents containing confidential information should be immediately removed from printers and fax machines.

Data Security

1. Personnel should use approved encrypted communication methods whenever sending confidential information over public computer networks (Internet).
2. Confidential information transmitted via USPS or other mail service must be secured.
3. Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
4. Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity.
5. Personnel should not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.
6. Confidential information must be transported either by an TCL employee or a courier approved by IT Management.
7. All electronic media containing confidential information must be securely disposed. Please contact IT for guidance or assistance.

Email and Electronic Communication

1. Auto-forwarding electronic messages outside the TCL internal systems is prohibited.
2. Electronic communications should not misrepresent the originator or TCL.
3. Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.
4. Accounts must not be shared without prior authorization from TCL IT, with the exception of calendars and related calendaring functions.
5. Employees should not use personal email accounts to send or receive TCL confidential information.
6. 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.
7. Personnel should only send confidential information using approved secure electronic messaging solutions.
8. Personnel should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
9. Personnel should use discretion in disclosing confidential or internal information in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information or other sensitive data.

Hardware and Software

1. All hardware must be formally approved by IT Management before being connected to TCL networks.
2. Software installed on TCL equipment must be approved by IT Management and installed by TCL IT personnel.
3. All TCL assets taken off-site should be physically secured at all times.
4. Personnel traveling to a High-Risk location, as defined by FBI and Office of Foreign Asset control, must contact IT for approval to travel with corporate assets.
5. Employees should not allow family members or other non-employees to access TCL information resources.

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 business-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 Internet.
   c. 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 of 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.
3. Systems Administrators, TCL IT, and other authorized TCL personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges should not access files and/or other information that is not specifically required to carry out an employment related task.

Security Training and Awareness

1. All new personnel must complete an approved security awareness training class prior to, or at least within 30 days of, being granted access to any TCL information resources.
2. All personnel must be provided with and acknowledge they have received and agree to adhere to the TCL Information Security Policies before they are granted to access to TCL information resources.

3. All personnel must complete the annual security awareness training.

Social Media

1. Communications made with respect to social media should be made in compliance with all applicable TCL policies.
2. Personnel are personally responsible for the content they publish online.
3. Creating any public social media account intended to represent TCL, including accounts that could reasonably be assumed to be an official TCL account, requires the permission of the TCL Public Relations Department.
4. When discussing TCL or TCL -related matters, you should:
    a. Identify yourself by name,
    b. Identify yourself as an TCL representative, and
    c. Make it clear that you are speaking for yourself and not on behalf of TCL, unless you have been explicitly approved to do so.
5. Personnel should not misrepresent their role at TCL.
6. When publishing TCL-relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer could be; “The opinions and content are my own and do not necessarily represent TCL’s position or opinion.”
7. Content posted online should not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws).
8. The use of discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances) in published content that is affiliated with TCL will not be tolerated.
9. Confidential information, internal communications and non-public financial or operational information may not be published online in any form.
10. Personal information belonging to customers may not be published online.
11. Personnel approved to post, review, or approve content on TCL social media sites must follow the TCL Social Media Management Procedures.

Voicemail

1. Personnel should use discretion in disclosing confidential or internal information in voicemail greetings, such as employment data, internal telephone numbers, location information or other sensitive data.
2. Personnel should not access another user’s voicemail account unless it has been explicitly authorized.
3. Personnel must not disclose confidential information in voicemail messages.

Incidental Use

1. As a convenience to TCL personnel, incidental use of Information Resources is permitted. The following restrictions apply:
    a. Incidental personal use of electronic communications, Internet access, fax

machines, printers, copiers, and so on, is restricted to TCL approved personnel; it does not extend to family members or other acquaintances.

   b. Incidental use should not result in direct costs to TCL.
   c. Incidental use should not interfere with the normal performance of an employee's work duties.
   d. No files or documents may be sent or received that may cause legal action against, or embarrassment to, TCL or its customers.

2. Storage of personal email messages, voice messages, files and documents within TCL Information Resources must be nominal
3. All information located on TCL Information Resources are owned by TCL may be subject to open records requests and may be accessed in accordance with this policy.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.