TRI-COUNTY TECHNICAL COLLEGE

PROCEDURE

PROCEDURE NUMBER: 4-4-1031.1

PAGE: 1 of 4

TITLE: Acceptable Use of Information Technology Resources

RELATED POLICIES AND PROCEDURES:

1 – 2 – 1030, Administrative Systems and Data Security Policy
1-2-1030.1, Administrative Systems and Data Security Procedure
1 – 8 – 1010, Reproduction of Copyrighted Print and Non-print Materials Policy
4-4-1010.2, Copyrighted Computer Software and Electronic Materials Procedure
4 – 4 – 1031, Acceptable Use of Information Technology Resources Policy
Tri County Technical College Cyber Security Incident Management Plan (Internal-Sensitive)

ADMINISTRATIVE RESPONSIBILITY: Vice President for Business Affairs

---

DATE APPROVED BY PRESIDENT: July 1, 2004

DATE LAST REVIEW: August 21, 2023

DATE LAST REVISION: August 21, 2023

Tri-County Technical College has established a series of procedural measures to oversee and maintain the integrity of its information technology (IT) resources. Below are the enforced procedures:

1. Addressing Suspected Violations

1.2 Should a policy violation occur, suspected to be attributable to a specific user, the user's authorizations will be immediately suspended. Both the user and their supervisor or instructor will be informed of the account suspension, which will remain in effect until due process is completed.

2. Investigation of Suspected Violations

2.1. All investigations into potential misuse of IT resources will aim to respect the roles and rights of all involved parties. However, the preservation of system, data, network integrity, as well as the safety of other campus users, takes precedence over the individual account access of the user(s) under suspicion.

2. Investigating suspected violations might necessitate inspecting data created, transmitted, or stored on College IT resources or network, may be conducted in consultation with the appropriate Vice President or Dean.

3. Ensuring Due Process for Policy Violations

3.1. Each policy violation will be referred to the appropriate Vice President or Dean, who will review the evidence in coordination with the Information Technology team and administer necessary disciplinary sanctions to guarantee policy adherence. IT may take specific action to protect the integrity of the Colleges systems and data. The user and their supervisor or instructor will be notified of this decision.

3.2 The decision of the Vice President or Dean may be appealed as prescribed by the College grievance policy for faculty and staff, or, in the case of student(s), the applicable appeal policy contained in the College Catalog for the current academic year.

4. Management of User IDs and Passwords

4.1 Access Code Sharing is Prohibited – Use of Tri-County Technical College computer accounts, user IDs, network passwords, voice mail box PINs, and other access codes is strictly limited to the individuals they are assigned to.

4.2 Sharing Passwords is Prohibited – Under no circumstance should passwords be shared or revealed to anyone other than the authorized user. Information Technology Department personnel will never request users to disclose their passwords.

4.3 Strong Passwords – Users must choose passwords that are difficult to guess and comply with all the Tri-County Technical college password guidelines.

4.4 Typing Passwords When Others Are Watching - Users should be aware of their surroundings and avoid typing their password at a keyboard or a telephone keypad if others are known to be watching their actions. To do so unduly exposes the information accessed thereby to unauthorized access.

4.5 Password Proximity to Access Devices - Writing down or recording passwords and storing them unsecured near the related access device is strictly prohibited.

4.6 Passwords in Communications Software - Storing fixed passwords in Internet browsers or any data communication software is forbidden.

4.7 Suspected Password Disclosure - If a password is suspected or known to be disclosed to an unauthorized party, users are obligated to change it immediately.

5. Security Incident Reporting

5.1 **Reporting Security Events** – All potential incidents that could threaten information security or known violations of existing security policies should be reported promptly to the IT department. These include, but are not limited to:

- Unauthorized use of Tri-County Technical College information systems;
- Loss, theft, or disclosure of passwords or other system access control mechanisms, or suspicion thereof;
- Unusual systems behavior, such as missing files, frequent crashes, and misrouted messages;
- Suspected or confirmed exposure of Sensitive Tri-County Technical College information to unauthorized third parties.

6. Privileged Access to College Resources

6.1 Training and Compliance Required – Users must complete **regulatory** mandatory training and achieve compliance before gaining privileged access to their accounts.

6.2 Re-Enforcement Training – Periodic retraining is necessary to retain privileged access to their accounts.

6.3 Knowledge Assessments – Routine knowledge assessments will be administered, with a satisfactory score or response. Failure to achieve a

passing score will necessitate further training to maintain privileged account access

6.4 **Compliance** - Failure to complete the requisite training will lead to the suspension of privileged access until training is fulfilled.