TRI-COUNTY TECHNICAL COLLEGE
STATEMENT OF POLICY

POLICY NUMBER: 4-4-1031

PAGE: 1 of 4

TITLE: Acceptable Use of Information Technology Resources

RELATED POLICIES
AND PROCEDURES: 1-8-1010, Reproduction of Copyrighted Print and Non-print Materials Policy

1-8-1010.1, Reproduction of Copyrighted Print Materials Procedure

1-8-1010.2, Reproduction of Copyrighted Non-print Materials Procedure

4-4-1031.1, Acceptable Use of Information Technology Resources Procedure

4-4-103, Internet Access (State Policy)

ADMINISTRATIVE
RESPONSIBILITY: Vice President for Business Affairs

October 12, 2020	October 2, 2023	October 2, 2023
DATE APPROVED BY AREA COMMISSION	**DATE LAST REVIEW**	**DATE LAST REVISION**

The use of information technology (IT) resources at Tri-County Technical College is a privilege, not a right. Abuse or misuse of College IT resources by administrators, faculty, staff, or students, or failure to comply with the provisions of this policy may lead to disciplinary action. Violation of federal or state legislation may result in criminal or civil action.

1.   **Unacceptable use of College IT resources includes:**

    1.1.   Violating federal or state laws, such as the Federal Copyright Law, the Family Education Rights and Privacy Act (FERPA) and the Gramm-Leach-Bliley Act.

    1.2.   Unauthorized accessing, copying, modifying, damaging, removing or distributing of restricted data and application software owned and licensed

---

by the College or any user data and application software without express permission the Chief Information Officer or designee.

1.3.   Deliberate removal, damage or alteration of College IT resources, or any intentional act that affects operational readiness, disrupts normal usage or restricts network access.

1.4.   Exploiting College IT resources for activities not relevant to College business or academic pursuit, including solicitation, personal financial gain or commercial advertising.

1.5.   Circumvention, or attempts to circumvent, any protective software or device installed on any College computer system, file server or workstation.

1.6.   Initiating, accessing, or reproducing offensive, harassing or libelous information on any College computer system, fileserver or workstation.

1.7.   Intentionally monopolizing IT resources to the detriment of others, such as by sending mass mailings or chain letters, generating superfluous output, causing unnecessary network traffic, or excessive printing.

1.8   College IT resources are primarily for College business use. Occasional incidental personal use is permitted, provided it does not interfere with business activities or IT resource availability.

1.9   Employees must utilize the College-provided e-mail for all business communications due to the potential sensitivity of the information. Redirecting email from the college provided email service to a personal email account is prohibited.

1.10   **Prohibited Use** — Use of the College's IT resources to send, view or download fraudulent, harassing, obscene, threatening, or any other content that violates applicable law or College policy, or contributes to a hostile academic or work environment, is prohibited.

2.   **User IDs and Passwords:**

POLICY NUMBER: 4-4-1031

PAGE: 3 of 4

2.1 **Personal User IDs and Passwords Responsibility** - Administrators, faculty, staff, and students, are responsible for all activity performed with their user ID. They must not allow others to use their user IDs or passwords and must not use IDs and passwords belonging to other users. Refer to procedure 4-4-1031.1.

3. Privacy related to IT resources:

3.1 **Privacy Legislation** — Information will be maintained and disclosed following all applicable state and federal laws to include the Family Educational Privacy Rights Act (FERPA), the Family Privacy Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and The Gramm-Leach-Bliley Act (GLBA).

3.2 Tri-County Technical College uses industry standard practices to monitor college-provided technology devices, software, tools, and network infrastructure. Given that IT resources are only to be used for legitimate business and academic purposes, the College reserves the right to monitor any activity or device utilizing the Colleges network, including individual personal computers, network drives, external storage devices, laptops and administrative systems, email, and individual documents. Investigations of this nature may be conducted in consultation with the Dean of Student Development for student-related offenses and with the Vice President for Human Resources for employee-related offenses. Consequently, neither employees nor students should expect privacy for data housed on their college-issued e-mail accounts or on college-owned computers.

4. Security Incident Reporting

4.1 **Reporting Security Events** – Any suspected events compromising information security or known violations of an existing security policy must be immediately reported to the IT department. Refer to procedure 4-4-1031.1.

5. Privileged Access to College Resources

POLICY NUMBER: 4-4-1031

PAGE: 4 of 4

5.1   **Training and Compliance Required** – Prior to granting privileged access to a user's account, mandatory cyber security training and where appropriate, federal compliance training must be completed. Refer to procedure 4-4-1031.1.