Procedure 7.4.1 Information Technology: Electronic Signatures

TRI-COUNTY	**INFORMATION TECHNOLOGY**	**PROCEDURE**
COMMUNITY COLLEGE	**ELECTRONIC SIGNATURES**	**7.4.1**

Tri-County Community College recognizes an electronic signature as a valid signature from faculty, staff, and students subject to the conditions below.

An electronic signature is defined as any electronic process signifying an approval to terms, and/or ensuring the integrity of the document, presented in electronic format.

Students may use electronic signatures to register, check financial aid awards, pay student bills, obtain unofficial transcripts, update contact information, log into campus computers, complete forms, or submit class work or tests.

Faculty and staff may use electronic signatures for submitting grades, viewing personal payroll data as well as logging into campus computers and accessing protected data through the administrative computing system and custom web applications provided by the college.

An electronic signature is considered valid when one of the following conditions is met:

Condition 1: Campus Network Username and Password

- Institution provides student or employee with a unique username
- Student or employee sets his or her own password
- Student or employee logs into the campus network and secure site using both the username and the password
- Network in this usage may refer to the College's networks, its Learning Management Software, its email system, or any TCCC data access portal.

Condition 2: E-mail confirmation

- E-mail message from student's TCCC email account to instructor/program director/coordinator indicating student's name and enrollment in the course.
- E-mail message from student's or employee's TCCC email account to other college personnel.

It is the responsibility and obligation of each individual to keep their password private so others cannot use their credentials. Once logged in, the student or employee is responsible for any information they provide, update, or remove. TCCC will take steps to ensure the password is protected and kept confidential. Furthermore, users are responsible for logging out of all systems and exercising the necessary precautions when using publicly accessible computers.

This policy is in addition to all applicable federal and state statutes, policies, guidelines, and standards.

Adopted: 8/23/12; 3/20/18 Technology Committee; 5/24/18 BOT