TOOELE TECHNICAL COLLEGE

# Safeguarding Consumer Information (PII) Policy

The College establishes and maintains a comprehensive information security program. This program includes the administrative, technical, or physical safeguards the school uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information. The safeguards achieve the following objectives:

- Insures the security and confidentiality of customer records and information
- Protects against any anticipated threats or hazards to the security or integrity of such records, and
- Protects against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer

Director of Information Technology (IT) oversees and manages a comprehensive information security program (including cybersecurity threats) that includes reasonable measures to secure customer information. The Director of IT regularly tests or otherwise monitors the effectiveness of the safeguards' key controls, systems and procedures; the Director provides employee training and management of information systems of storage and transmittal of confidential information; the Director changes password codes to network systems and shares with staff members who need access to the system; the Director contacts all service providers in the event of a breach of security.

Student Services staff ensures any document with a student's PII, either electronic or paper, is not within viewing site of the public and secured at night. Staff ensure the Records Room is locked at all times and student files are locked each night. Staff ensure that access to the student education records is limited to authorized personnel (student services and College administration).

All staff are responsible learn and follow safeguards that are identified in this policy. Staff ensure that unneeded documents containing student performance, social security numbers, or other personal information are shredded (shedder located in Student Services records room). Staff ensure that all passwords are secure and will not share their password. Staff remember to log out of all computers and programs that allows access to the SIS or other document with PII. Staff do not allow their computer screen to be viewed by members of the public or by school officials who do not have a legitimate educational interest.