TCR TECHNICAL COLLEGE OF THE ROCKIES
Where Careers Begin

Protection of the Intuition's Technical Infrastructure Plan

Purpose

Technical College of the Rockies is committed to ensuring the privacy, safety, and security of data contained within the technical infrastructure of the institutional network.

This plan is distributed and reviewed annually by staff, faculty, and students through student surveys and staff/faculty meetings. The plan is available on the TCR website.

Privacy, Safety, and Security of Data

Technical College of the Rockies complies with Title 17 of the United States Code and Title IV of the Higher Education Opportunity Act. The institution's computers are connected to the network provided by the Delta County School District via their contract with Elevate Internet.

Technical College of the Rockies online application has been configured so that social security numbers, home addresses, telephone numbers, and other personal information is not stored locally. Because this information is not stored on the system, student data is adequately protected against the theft of sensitive information. The filters from the Google for Enterprise Pro email server provides protection against viruses, malware, spam, phishing, pharming, and other threats to most email accounts.

The institution's servers are housed in a room, located on the main campus in the Delta County School District IT Department, which is always locked. Access to the equipment room is limited to TCR and DCSD IT authorized personnel only. The department is secured with an alarm system from an outside service for protection in the off hours.

Secured data storage is on high-availability data security using RAID 5 protection. Data is backed up at TCR and the North Fork High School campus located at 438 Miners Way, Hotchkiss, CO 81419, creating an internal redundant backup set of data. Therefore, if one site has a fire, all data will still be safe from loss. Essentially, two backup copies of data will be stored at the very least. Backups used are shadow copy, RAID, and stand-alone RAID. Data is backed up automatically nightly and on a weekly basis. Cloud based services are backed up within the subscribed company (Sonis, Open LMS).

These file servers also have a snapshot capability used for quick access to storage checkpoints. Snapshots are near-instantaneous, transparent, read-only, online copies of the active file systems, and IT staff can quickly recover deleted or modified files without the need to restore from tape backups that are stored offsite. Snapshots are performed daily and kept for up to 7 days.

Password protection is implemented in layers. Everyone has password access to the computer they use. A 9 -character password that changes once per year. As another level of security, staff is given access to only the servers or permissions for their program or job requirements. New security requirements are being implemented for higher risk services such as finance and admin level server management by adding MFA (multi-factor authentication). All student accounts are deactivated on the last day of June every year. An employee who leaves has their account deactivated and all access is removed immediately.

Technical College of the Rockies has an infrastructure in place for distance education programs to ensure the system is secure, reliable, safe, and private in regard to student records. Online login information is password protected and on a secure server hosted and maintained by Open LMS which is our third party Moodle provider. Access to student's credit card, social security numbers and other theft sensitive information is not accessible in the Moodle system since registration for programs is done through SONIS, our student information system.

TCR has processes in place to establish that the student who registers for a distance education course is the same student who participates in and completes the course and receives the academic credit. A student enrolling in an online course as part of an online/hybrid program is added to the course roster after the program registration process has been completed in the Admissions Office. Each student receives a unique ID from SONIS which is used to create the login and password for Moodle. Students are notified that interactions with Moodle are recorded in log files including student name, date, time, IP address, activities, and actions. This will allow instructors to use data from log files to check the student's IP address during proctored exams. Proctored exams use a password to access it. The password is provided by the instructor. Instructors will use various techniques to limit cheating on exams such as randomized questions, multiple questions from pools, time limits, limited availability, and proctored exams.

Hard copy records that must be retained for certain programs are stored in a fire-proof vault that has restricted access.

Revised on 1/11/2022 by Tony Bowling, Assistant Director, and Lisa Harris, Student Services Coordinator, based on input from staff meeting held on 1/3/2022.