



Technical Infrastructure Plan

SCOPE OF SERVICES

The objective of this plan is to ensure that TCAT Elizabethton has reliable technical infrastructure and to protect private data.

Person(s) responsible:

The college IT department.

Adequacy, Improvements, and Protection

- Technical infrastructure will be upgraded or replaced as needed to ensure it adequately supports the college's mission.
- The college IT department will stay up to date on current technology and the needs of the college to identify necessary improvements to the technical infrastructure.
- Servers and network equipment are physically secured in locked rooms or cabinets to prevent unauthorized access. Student and staff networks are segregated using VLANs. Servers and network equipment are password protected and accessible only by the college IT department.
- TBR operates and makes needed improvements to D2L for distance learning.

Operation and Maintenance

- Ongoing operation and maintenance of TCAT Elizabethton's technical infrastructure is provided by the college IT department. Tennessee Board of Regents (TBR) IT staff assist as needed.
- Distance learning is available through D2L, which is operated by TBR.

Privacy, Safety, and Security of Institutional Data

- Legacy student records are stored in the cloud-based Argos system and are secured and maintained by TBR. Additional scanned copies of legacy student records are securely stored on a Teams file share.
- Paper copies of student records are kept secure as well. All required paperwork is placed in the students' file. Student records are securely stored in the fireproof vault. Student records are maintained until the student is terminated from or completes their program. Disposed records will be shredded. Electronic copies of the students' transcripts and their diplomas will be available from TBR through Banner.
- Network security is provided by TBR through firewalls installed at each campus.
- In the event of a suspected or confirmed cybersecurity incident, TCAT Elizabethton will follow the Tennessee Board of Regents (TBR) Cyber Incident Response Plan and coordinate all response activities with TBR Information Technology in accordance with established TBR policies and procedures.



Computer and Network Reliability

- Servers and network equipment are powered by UPS units for surge protection and battery backup in case of power failure.
- Servers and network equipment are physically secured in locked rooms or cabinets to prevent unauthorized access.
- The college IT department repairs malfunctioning computers or sends them to the manufacturer for repair.

Evaluation and Review

- The college IT department continually monitors and evaluates the college's technical infrastructure to identify any improvements or issues.
- The college IT department reviews this plan annually and makes revisions as needed.

Budgetary Review

- Our Technical Infrastructure undergoes an annual budgetary review process, incorporating input from faculty and staff, to evaluate and allocate resources effectively, ensuring we meet both our operational needs and strategic goals.

Technical Infrastructure Plan Availability

- The technical plan for the college is contained in the faculty handbook which is revised annually. The faculty handbook is distributed to all faculty and staff when revisions are made.