Lancaster County Career & Technology Center (LCCTC)

Technical Infrastructure Plan

Purpose

This plan defines the policies and operational framework to maintain, evaluate, and enhance the technical infrastructure at LCCTC in full alignment with COE Standard 6, Section C. It ensures adequacy, improvement, protection, and maintenance of the institution's technological environment, including provisions for privacy, safety, and security.

Scope

This plan applies to all LCCTC campuses, personnel, students, and third-party providers engaged in the use or support of institutional technology systems.

1. Plan Development and Implementation

LCCTC maintains and implements an institution-wide Technical Infrastructure Plan that:

- Documents system-wide standards for network, hardware, software, and instructional technologies.
- Aligns technology strategy with institutional goals, instructional programs, and COE compliance.
- Is distributed to administrative leadership, faculty, and relevant staff.

2. Adequacy, Improvements, and Protection

LCCTC ensures adequacy and protection of technical infrastructure through:

- Annual audits of instructional and administrative hardware/software against program requirements.
- Lifecycle planning for replacements (typically 4–5 years) using inventory and help desk data.
- Strategic upgrades driven by faculty feedback, emerging industry standards, and enrollment changes.
- Cybersecurity protocols including:
- Multi-factor authentication for administrative systems
- Next-generation firewalls with active monitoring
- Role-based access and data encryption (at rest and in transit)
- Incident response protocols reviewed annually

3. Operation and Maintenance

Ongoing technical infrastructure operations include:

- Centralized IT help desk support (in-person, virtual, and ticket-based)
- Weekly and monthly maintenance schedules for systems, servers, and cloud services
- System performance monitoring (uptime, usage, load balancing)
- Instructional technology coaches providing training and support for faculty

4. Privacy, Safety, and Security of Institutional Data

- Data access is restricted using least-privilege principles.
- Student and staff records are encrypted and stored in secure cloud environments.
- All personnel complete annual cybersecurity and FERPA compliance training.
- The IT team responds to security incidents per the Disaster Recovery Plan (DRP).

5. System and Network Reliability

- Network uptime is measured and reported quarterly.
- Redundant systems ensure continuity of service in instruction and administration.
- Cloud-based learning platforms and secure content delivery minimize outages.
- Offsite backups and regular testing of failover systems support reliability.

6. Annual Evaluation and Revision

- The Technical Infrastructure Plan undergoes formal annual review.
- Data sources include system performance logs, stakeholder surveys, and audit results.
- Revised plans are disseminated to stakeholders and incorporated into the LCCTC Strategic Plan.

7. Plan Accessibility

- Summary documentation of the plan is available on the LCCTC staff intranet.
- Department leads receive printed and digital versions.
- Orientation materials and staff meetings incorporate plan highlights annually.

8. Accessibility of Technology for Instructional Delivery

- LMS and digital tools are selected to avoid accessibility barriers.
- Secure platforms (e.g., Zoom for Education, Teams) are utilized for distance learning.
- Virtual assessments incorporate proctoring tools and student ID verification.
- Technology use is reviewed for equity across student populations.

9. Protection of Student Coursework and Records

- Coursework submitted via LMS is archived for backup and audit purposes.
- - Testing records are encrypted and access-controlled.
- - Regular audits validate data preservation in compliance with FERPA and state requirements.