Technical Infrastructure Plan
2025 - 2026

Introduction

Miami Lakes Technical Education and Technical College has developed a technical infrastructure plan to address and maintain the adequacy and improvement of the school's technical infrastructure. The school is committed to safeguard the data stored on the school network and supply safe, secure, reliable network access to the faculty, staff, and students.

Ongoing Operation and Maintenance

Students attend an orientation session conducted by the Media Specialist regarding the use of technology in the school, whether in the classroom or the media center. Employees are given levels of access by the school director according to their roles and responsibilities. Each employee with access to confidential information is assigned a username and password. All databases and imaged documents containing confidential information are password-protected and it takes reasonable and appropriate steps consistent with current technological developments to ensure that all sensitive data are secure, and to protect the integrity of records in storage and transmission. The technology inventory of the various computer labs in the technical shops, the classrooms, and the media center indicate that students have access and adequate support to technology at MLEC&TC.

All employees and students at Miami Lakes Education Center and Technical College are expected to adhere to the Miami-Dade Public Schools' Acceptable Use Policy; any violation of the policies and procedures may lead to suspension of network privileges, and/or termination of employment for employees, and expulsion for students.

Personnel Providing Computer System and Network Reliability

The Miami-Dade County Public School IT department assigns a full-time Computer Systems/ Information Technology technician who works under the supervision of an assistant director to perform the following tasks:

- Ensure adequate Privacy, Safety, and Security of Data Maintain server access

- Perform periodic network scans for suspicious, questionable, disallowed, or potentially copyright-infringing files

- Require universal strong passwords

- Monitor web and network traffic, the firewall, web filtering logs, and spam filter for anomalies.

- Follow formal security, data retention, and disaster recovery policies. Maintain

a list of supported software and track installed applications

- Schedule internally hosted automated remote patch installation on workstations and automated patch awareness on servers

- Continue to monitor wireless networks and the current rogue tracking and containment process

Technology Support and Data Security

The Computer Systems Technician is responsible for ensuring privacy, security, reliability, and backup of all network data. Responsibilities also include managing software licenses, maintaining and repairing computer systems and network infrastructure, overseeing records storage, and safeguarding student confidentiality in accordance with all applicable regulations.

Plan Evaluation

The Technical Infrastructure Plan is reviewed annually during the Opening of Schools meeting. Following the evaluation, revisions are made as needed. A copy of the current plan is available in the offices of the school administrators, the Computer Systems Technician, the media center, and the program chairpersons.