Tri-County Career Center Privacy, Safety and Security of DATA with the Technical Infrastructure Plan

Privacy, Safety and Security of DATA with the Technical Infrastructure Plan

Tri-County Career Center strives to provide a top notch technology department. The center has protocols in place that protect the data on the servers and computers. The center has plans in place to protect the safety of the buildings.

The center employees a full time IT Staff to maintain technical infrastructure – This department oversees the Firewall, Servers, Google Workspace, and all aspects of protecting the DATA of our center and students. Tri-County Career Center maintains a hybrid Windows Server and Google Workspace infrastructure for all computing, email, and storage needs. On-premises servers house most staff files, while students utilize Google Drive for personal storage. Staff are given the option to use both on-premises storage and Google Drive. The center has an iBoss content filter and Thirtyseven4 EDR software firewall to ensure the privacy, safety, and security of the data that is contained on the district servers and computers. ThirySeven4's EDR software also ensures that every district server and computer are protected from malware, viruses, and phishing attempts. These devices and software ensure CIPA compliance on the network, as well as protecting district computers from dangerous viruses and malicious content. Our Internet Provider also has Firewalls and security policies in place to protect the center.

All servers and network equipment have a battery backup system connected to them that ensures at least an hour of runtime in the event of a power failure. Backup power will allow all core network equipment to run for a minimum of 45 minutes to allow our technical staff to safely shut down all equipment in the event of a power failure.

The staff is trained on the importance of keeping their passwords secure. All passwords are required to be reset every 120 days. Passwords may not be reused and must meet complexity requirements to be allowed to be used as a password.

Virtual servers, storage data, and Google Drive cloud are backed up daily to a storage appliance in our second building. These backups are replicated daily to an off-site storage appliance housed at our Internet Provider's location.

Tri-County Career Center Privacy, Safety and Security of DATA with the Technical Infrastructure Plan

There is a developed technology infrastructure with plans of replacement and deployment of new technology. Each program has ample technology to meet their needs. Most are replaced on a five-year replacement schedule.

Procedures and Specific Guidelines

All new technology expenditures are approved by the Director and Superintendent. There is an advisory board that gives advice on the center's technology needs. The center continues to evaluate the need to increase the bandwidth. This is evaluated on an annual basis. Software and hardware purchases have to be approved by the Technology Coordinator, then the Director and Superintendent.

The center has a content filter to ensure the privacy, safety, and security of the data that is contained on the district's servers and computers. The district also ThirtySeven4 endpoint detection and response, firewall, virus and malware protection software on every district Windows and Mac computer. Chrome devices are protected by Securly Filter, a web filter software, when off-premises. These devices and software ensure CIPA compliance on the network, as well as protect district computers from dangerous viruses and malicious content.

Servers at the center are replaced on different schedules depending on what the server is used for. Tier 1 servers (primary servers) are Hypervisor hosts that house all virtual servers. Tier 2 servers are usually replaced on a 5-7 year rotation, or upon failure. Tier 2 servers are purpose built for applications or services such as our security camera storage server and door access controller.

We have several procedures in place to deal with repairs throughout the center. Helpdesk software is utilized for request ticketing should a user have a technology problem. An email to our helpdesk submits a ticket in the system. Having this ticket allows the technology department to keep track of the repair(s), keeps the user informed of repair status, and allows better efficiency in day-to-day operations.

Tri-County Career Center Privacy, Safety and Security of DATA with the Technical Infrastructure Plan

Every student and staff are required to complete an Internet User Agreement before they have access to the center's computer system. Once a signed user agreement is returned, the staff or student account is enabled and that user is allowed to access the network or use their Google account. In addition to cloud storage in Google Drive, each network user is granted a secure on-premises network share where they can store files or use it as a means of backup. The users are only given access to their share unless otherwise needed for their job duties and approved by the administration. These file servers are backed-up every night in a separate building than the originating server.

Staff, students, and guests are permitted to bring personal devices on our network. Strict wireless policies ensure core network is kept separate from personal devices. Plugging personal devices physically into the network is strictly prohibited. Personal devices do not have access to the center's network but rather just plain internet access.

COE Standards – 6.16 - 6.21

Created 03.01.2017
Revised 03.07.2022
Revised 05.17.2023