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 recently undergone a huge renovation that protects the safety of the buildings.

The center employees a full time IT Staff to maintain technical infrastructure – This individual is in charge of the Firewall, Servers, and all aspects of protecting the DATA of our center and students. Tri-County Career Center maintains a secure Windows Server based network for all storage needs. These servers include house both student and staff files. The center has a Barracuda firewall and web filter to ensure the privacy, safety, and security of the data that is contained on the districts servers and computers. The district also deploys Sophos virus and malware protection software on every district computer. These devices and software ensure CIPA compliance on the network, as well as protects 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 60 days. Passwords may not be reused and must meet complexity requirements to be allowed to be used as a password.

All technology is secure and has a backup procedure daily. The backup in maintained in both buildings.

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 firewall and web filter to ensure the privacy, safety, and security of the data that is contained on the district's servers and computers. The district also deploys Sophos virus and malware protection software on every district computer. 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) that handle our daily network functions such as active directory, DNS, DHCP, staff and student files are replaced every 5 years or sooner if a failure occurs. Tier 2 servers are usually replaced on a 5-7 year rotation. Tier 2 servers are servers that are not vital to the daily operation of the center.

We have several procedures in place to deal with repairs throughout the center. A helpdesk program allows users to submit a ticket with their technology problem. This program allows communication throughout the repair. The staff is required to complete a helpdesk ticket if any technology assistance is needed. A helpdesk ticket is created by sending a detailed email of the problem to the helpdesk server. The helpdesk system allows the technology staff to keep

organized and keep track of technology problems throughout the center and also allows for notification emails to be sent to the originator of the tickets on the progress or status.

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. Each network user is granted a 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.

We require staff and students that bring their own devices to sign into our wireless network each day so we know who is using what device. We also have a strict virus scan policy where each device must be scanned before it is allowed on the wireless network. Plugging devices directly into a network drop is strictly prohibited. Guest and student wireless access are separated from the rest of the network via firewall policies to ensure the integrity and security of the center's network. Personal devices do not have access to the center's network but rather just plain internet access.

COE Standards – 6.