Tri-County Regional Vocational Technical School District
General Policy for Data Privacy and Network Security

Overview

Data privacy and network security are recognized are essential elements in the general operation of the Tri-County Regional Vocational Technical School District. In order to meet these obligations as they apply to our stakeholders, both internal and external, we have in place many industry standard controls. These controls typically fall into one of three categories, administrative, technical, or physical.

Administrative Controls

Within the category of administrative controls, we have in place acceptable use polices that establish the guidelines for expected employee behavior as it pertains to the data systems necessary to perform their duties. These polices include, Network and Internet Use, Email Use, and Social Media Use. Employees are trained in the concepts of data privacy and the government regulations that apply to their handling of data based on a particular job function. Employees are instructed as to the necessity of strong passwords and the avoidance poor practices such as password sharing.

Technical Controls

In order to mitigate threats to data privacy and network security, a layered "defense in depth" approach has been adopted. This layered approach includes a number of physical devices placed at key locations within the network architecture. Located at the Internet edge, a Unified Threat Management (UTM) appliance mitigates remote threats. Downstream from that device is a dedicated hardware based firewall that further inspects all inbound traffic. All user endpoint devices are subject to Internet traffic filtering based on both URL category and application category. Additionally, reputation based criteria is employed to augment these methods. Internal network access to data is controlled based on user roles and device location. The principal of least privilege is also employed. All user endpoint devices are equipment with centrally managed anti-virus, anti-spyware, and host based intrusion prevention software. All email traffic passes through an email gateway that applies anti-virus, anti-spam, and reputation based inspection and filtering.

Physical Security

All servers and data storage, core and access layer network switching, and staff workstations have been secured in areas where access is limited by locked doors, accessible to authorized personnel only.