SARASOTA COUNTY SCHOOLS

SUNCOAST TECHNICAL COLLEGE

PRIVACY, SAFETY, & SECURITY OF DATA WITH THE TECHNICAL INFRASTRUCTURE PLAN

REVISED: 1/23/2017

SECTIONS

1. Data Storage & Network Access

STC's IT staff manages all staff and student access to our domain and networks. They work closely with district IT staff to ensure STC is operating with a safe and adequate infrastructure. Further, the STC network manager holds Microsoft Certified Solutions Expert (MCSE) credentials in the following areas: server infrastructure, desktop infrastructure, private cloud, enterprise devised and apps, data platform, business intelligence, messaging, communication, and SharePoint. This allows our IT staff to have direct knowledge regarding Microsoft's best practices in technology infrastructure.

STC employees and students are provided with credentials to access the STC network and provided server space to store digital materials. When an employee is no longer a staff member or when a student is no longer enrolled, their access to the server and network is revoked.

2. Privacy, Safety, & Security

Application and User Security

User Authentication: User data on our database is logically segregated by account based access rules. User accounts have unique usernames and passwords that must be entered each time a user logs on.

User Passwords: User application passwords have minimum complexity requirements.

Data Encryption: Certain sensitive user data, such as account passwords, are stored in encrypted format.

Physical Security

Data Centers: STC's information systems infrastructure (servers, networking equipment, etc.) are located in a key-card access only locked area. STC owns and manages all equipment located in our data center.

Data Center Security: STC's data center is surveilled 24 hours a day, 7 days a week. Access is fully secured with key card entry requirements and entry logs are stored by key cards used.

Environmental Controls: STC's data center is maintained at controlled temperatures and humidity ranges which are continuously monitored for variations. Smoke and fire detection and response systems are in place.

Back-Ups: Back-Ups are performed on a daily basis. All back-ups run a 3-week cycle with storage on and also off-site.