

Tk20 Security Document for Data Security

Tk20 takes the following steps to ensure security of data belonging to its clients:

- All servers run the Linux operating system, a far more secure operating system than Windows with respect to system intrusions, trojans and viruses.
- Data from each individual client is housed in a separate server. Tk20 does not house data from multiple clients on the same server.
- Tk20's application has an N-tier architecture. The database has its own separate tier and is isolated from the rest of the application. Only the application tier has authorization to access the database, leading to complete data isolation and security. All connections to the database are authenticated with respect to authorization for access.
- All password and social security information is encrypted in the database.
- All communication between users and the application is encrypted. Tk20's application URL starts with the https protocol.
- All servers are protected behind a Cisco 506E firewall.
- All servers are continuously monitored for proper and expected operation.
- Servers are housed in a secure data center. Access to the data center and the servers is strictly controlled. The center has smoke detection, continuous power arrangement, a Liebert system and battery backups. The center has multiple T1 connections from independent sources.
- All data is backed up daily on hard drives. Backed up data is transferred weekly onto tapes. The tapes are stored in a separate facility from the servers.

Tk20 compliance with FERPA regulation requirements

Data is fully compliant with FERPA requirements. You will be transferring data from your other systems to one of your own systems. Tk20 will be merely your agent and administrator for system management