STAGES Security Statement

Application Security

STAGES Software utilizes the most widely used security measures available to internet applications. STAGES data communication is encrypted with a 256-bit SSL certificate. This is the same level of encryption that banks and other financial institutions use to encrypt their data communication. In addition to the standard encryption method all STAGES users are forced to login using an email address and password to gain access to the software. STAGES has been engineered with multiple access levels. Users are granted the appropriated access by their Institution's STAGES Database Administrator.

Physical Security

STAGES servers are physically hosted in a modern lights out datacenter located in Michigan, USA. The datacenter is fed by a standard AT&T DS3 type internet connection. Entry to the datacenter is only granted to server administrators. Backups to the database and STAGES code are saved onsite in the datacenter on a separate backup server and offsite in a remote datacenter location. Backup methods are all fully secured and encrypted between the datacenter and remote datacenter locations using a private backhaul connection.