



## mentorPRO system security

---

### **Security**

MentorPRO employs a username/password model to control data access within organizations and programs contained in the MentorPRO database. Secure Sockets Layer (SSL) technology is also used to encrypt all data transmission. SSL technology relies on the concept of “public key cryptography” to accomplish its tasks.

### **Data Protection, Redundancy and Backups**

Firewall technology is used to block unauthorized connection attempts to the servers over the Internet to gain access to the application and data. The application and data servers’ Operating System software (Microsoft Windows Server 2003) is constantly updated with security patches as they are available. In addition, an outside firm is used to test outside connections on a regular basis to ensure that the application/data servers are protected from all known vulnerabilities.

The application and data servers are equipped with Redundant Array of Independent Disks (RAID) hard drive architecture to ensure data integrity. The MentorPRO Web site and database is backed up nightly, so the data could be restored to an alternate server within a few hours if a catastrophic incident occurred.

### **Database Server and Capacity**

Microsoft’s SQL Server 2005 is used to store all data within the MentorPRO application. The current capacity of a SQL Server database (over 1 million terabytes) is governed only by the size/capacity of the server equipment it runs on. Further, the SQL Server RDBMS (Relations Database Management System) provides for both scaling up and scaling out.