St. Peter's Business Services
Data Safety and Security

Security Procedures

Data for a congregation is maintained in a commercial accounting system from ACS Technologies on a Windows Server system. Each congregation's data is in a separate set of files with a password unique from all other data sets. The computers are in a locked and alarmed office, and the servers in another locked and alarmed room with a more restricted key than the office. Recorded video surveillance is active both inside and outside the building. Each user of the computer system has their own login id, validated by Active Directory and changed at least every six months. The file system has its own access permissions using standard windows Active Directory mechanisms. The data base has a separate login ID/password for each user and users are restricted to access only the data sets they need. VPN remote access is not installed.

Data submitted as part of the financial record keeping process is stored as scanned/PDF documents on the file system and not retained in paper form. That data is protected by the operating system, file system, and physical security measures. All papers that contain confidential information (like bank account numbers, SSN's, etc), are shredded. All reports are stored on the file system as Word, Excel, and/or PDF documents. The final year-end CD to the congregation for the year's records will contain these files, and so that CD should be stored in an appropriate manner by the congregation.

Backup Procedures.

Computer data is stored on a Windows Server system. All files are on a main server and never stored on a workstation. That server is mirrored to a second server each evening. Each accounting database is also archived to a zipped file each evening, using a rolling set of 12 files, and providing the ability to recover a specific dataset up to 12 days after the causative event.

The entire system is backed up to DAT tape every weekend to a rolling set of 15 tapes, providing the ability to recover to a specific point up to 15 weeks in the past. The most recent backup tape is stored offsite, and other tapes stored with the servers. Tape backup is autoverified and also manually checked for readability every six months.

For long term backup, the entire system is archived to DVD every six months, one set stored with the servers and a second archive set stored off site. Finally, St. Peter's Business Services maintains a contract with the accounting software vendor to provide database reconstruction service should a significant corruption be discovered that cannot be readily corrected with backups. We have used this service only twice over the last decade and found it both useful and prompt.

August 4, 2011