



How Secure is Your Vital Information?

➔ There When You Need It

Churches amass considerable amounts of data whether they realize it or not, including attendance records, membership rolls, visitor addresses, vendor relationships, giving patterns, sermon audio files, capital campaign data – even lists of cemetery plots on church property.

Losing this information could cripple a ministry. With smart viruses, hackers, electrical surges, and natural disasters bearing down on you, consider implementing a systematic, efficient data backup system. To help you through this process, ACS Technologies' top experts answer the most frequently asked questions.

"...churches amass considerable amounts of data... membership rolls... giving patterns... capital campaign data.... Losing this information could cripple a ministry."

➔ At what point should our ministry consider implementing a data backup system?

Ministries use different criteria to determine the right time to start backing up their data. Some use a size threshold (e.g. 512 MB or 1G) of storage space being used on their computer system. Some use a certain number of members before they begin thinking about data security. Of course, budget and time also play active roles in the decision making process. Often the perceived low cost of CD backups outweighs the decision to set up and implement an automatic backup system. In addition, the urgent duties of daily life often leave the task of CD backups as an optional activity at the end of the day. In the event of an emergency, this could be potentially devastating.

The primary consideration for backing up data should be the cost to replace the data files if they are lost. Imagine the costs for researching alone – dispatching a team of administrative workers to comb through old paper files and church directories; making several weeks worth of phone calls; constructing new databases of addresses, phone numbers, and birthdays.

What's more, all the basic membership data mentioned above doesn't take into consideration the all-important financial information, giving data, or capital campaign records. Then there's the payroll data – do you want your accounting department spending valuable time reconstructing payroll information?

➔ Which files should we back up?

We are living in the age of information where the movement of information has become faster than physical movement. Arguably, information is your most valuable asset. It is this vital information that you want to keep as secure as possible. It includes names of your members, large donors, staff members, teachers, volunteers, community influencers, associations, vendors – as well as all of their contact information.



Testimonial

LiveStor™ Provides Data Shelter in Time of Storm:

On Friday, Aug. 26, 2005, Joann from St. Andrew Baptist Church in Panama City, FL, heeded the weather reports about imminent stormy weather. Wanting to protect her critical data, she called LiveStor Support at ACS Technologies to review her backup plan.

Normally, Joann's ACS automatic backup and LiveStor jobs run around 10 p.m. Her most recent ACS backup was just stored on the LiveStor server the previous night. Joann considered her options. Before she left the office, she could run both backups, confirm that they were successful, and power down her computer. Or, she could let the jobs run at their scheduled times. In the event that electrical power was lost and the jobs could not run, Joann could lose the day's work.

Joann didn't think they would lose power. She opted to leave the computers powered up and let the jobs run at their scheduled times. However, she liked the idea of checking on her jobs over the weekend. The next morning, from her home computer, she visited the LiveStor Administration Web page, entered her secure LiveStor username and password, and verified that her ACS backup zip file from the night before was successfully stored on the LiveStor server.

The next Monday, Joann called ACS Support to say that she liked the flexibility that LiveStor provided. Being able to check on her backups from home gave her the peace of mind that she needed.

The data includes all of your ministry's financial records, including giving patterns, special offerings, budget goals, salary records, annual forecasts, campaign contributions, tax returns and payroll information – all the information you use to make decisions about the direction of your ministry.

Graphic files are also very important. Imagine having to pay a designer to reconstruct all of your ministry's art files – logos, brochures, bulletins, stationery, business cards, newsletters and Web site pages.

Many ask, "What about the application files, such as Microsoft Word and Excel program files, we use? Should we duplicate those, too?" This answer may surprise you, but no. Keep the original application file CDs in a safe place – you can even make a couple of backup copies if you desire – but application files do not grow and change like data files. One hint, however, if you do make copies of your application and executable files, make sure you attach any passwords or security keys to the copies as well as the originals.

➔ **How frequently and when should I backup my data, and how long should my data files be stored?**

Backups can be either automatic – performed unattended at scheduled, predetermined times – or manual. It's important that you have the option of doing either. For example, if your local weather forecast calls for thunder storms and your last automatic backup was two days ago, you should have the option of manually backing up the data before the storm arrives.

Most people schedule their backups to run unattended after working hours. With LiveStor, you can easily run your scheduled backup jobs any time you want. This is important for those times when you don't want to leave your computers turned on or, you can let your jobs run as scheduled and check the results by visiting the LiveStor Administration Web page.

With scheduling any kind of backups ,automatic or manual, determine how long it would take to recreate the data if it were lost; then make your decision based on that. If your staff could recreate or reenter data from several days relatively easily, then schedule backups to run two or three times a week. For larger, multi-faceted ministries who gather and enter significant amounts of data on a daily basis, then daily data backups make sense. As for time of day, automatic backups run best after hours, when fewer demands are being made on the computer system. Performing after-hours backups also lessens the chances of attempting to secure open files – many systems recognize opened files as locked files and will not back them up.

Also, consider backing up data prior to significant events, such as closing out yearend data or before significant system upgrades.

➔ What kind of media should we use for backups?

The type of media such as tapes and CD, used affects the security and accessibility of your data. There are advantages and disadvantages to every media. Whatever you use, the primary consideration in the case of massive data loss, such as in a virus attack, electrical storm or hurricane, is your ability to get up and running quickly, which can make or break the survival of your organization.

If your church uses physical media for local backups (tapes, CDs or DVDs), make sure to maintain a consistent schedule for backing up data. With this type of manual backup system, it is best to name one person responsible for performing all duties relating to the backup – purchasing the media, cleaning tape drives, backing up the system, logging the backups and transporting/storing the tapes or disks. This administrator must also be able to manage the task of restoring files to the server if the worst should happen.

Taking a look at the above scenario, several questions arise:

- What if something happens to the person responsible for backing up the system, especially while transporting/storing the data files?
- If a natural disaster hits our city or town, is our information not vulnerable, both on- and off-site? Then isn't a local backup and storage system a gamble?
- Purchasing tapes, CDs and DVDs cost money. These systems also require their own storage space in our facility, as well as regular maintenance on the equipment to keep it running properly. Is there a way to control costs, reduce maintenance, and get the same reliability?

These are all good questions. Many ministries have found a viable alternative through virtual backups via the Internet. These regularly scheduled, automatic backups can transmit your valuable data – securely – to remote servers in another part of the country. You can schedule them as frequently – or infrequently – as you want and set them to run “in the background” without interrupting normal work. Costs are usually based on the amount of storage on the remote server. Local equipment maintenance is usually limited to providing a reliable Internet connection. Local administrative requirements are minimal. There is no ongoing cost for media, no extra physical storage space necessary and no maintenance to worry about.

➔ Won't my data be vulnerable if I transmit it over the Internet?

Ministries assume some level of risk with any form of data transmission and storage, however, a virtual backup through the Internet to secure off-site servers is one of the safest ways to ensure the integrity of your data. Traditional media such as tapes, CDs, and DVDs could be accidentally erased, destroyed, or thrown away, or worse, stolen.

While Internet security has many times fallen victim to sophisticated hackers, software and hardware companies are generally staying one step ahead of the efforts to steal valuable data. Today's encryption processes are constantly being updated and improved to make it increasingly difficult for hackers to break through.



Once your data is securely stored on off-site servers, it should be available only to the person in your organization responsible for the backups and the vendor's server administrator should it become necessary to restore the data. The vendor should also submit and adhere to a very strict privacy policy before any data is transmitted.

➡ How is our information restored, if the worst should happen?

Depending on the backup system you choose, you should be able to restore a single data file, multiple files, single folders, multiple folders, an entire drive, or every file you have stored. In the case of a complete hard drive crash or other event that wipes out your system, reinstall your operating system and application files first, using the original application disks.

After reinstalling the applications, restore your data files from physical media or virtual file storage. If you have used offsite servers to secure your data, use your offsite service's "Restore" function to restore your data. With one download, the restore program should allow you to restore the files to the original location on your server or hard drive. Once data files are restored to your computer, you can access the files by opening them in the appropriate application.

For specific applications that include a backup function, always perform that function first. Many financial applications offer this feature. Once you have used the application's backup function, store just those backups offsite. Usually, the specific application backup creates a zipped or compressed file of the data. In the event that a restore is needed, first restore the backup zip file to the local computer using the offsite service restore function. Then, in order for the data to be accessible by the specific application, perform the specific application's restore function.

If your original computers were damaged beyond restoration, you should be able to restore the stored data to another computer with the same applications installed.

➡ What kind of data security partner should I be looking for?

There are many partners who can supply your needs when it comes to data security. Therefore, take great care when selecting a partner. Choose a partner that:

- **Understands your needs.** Many software solutions are available, including those offered by large, big name companies who can provide lots of options. While a popular option, churches and other ministries have unique needs that these products are not familiar with. Attend user conferences and listen closely to management's direction for the company.
- **Offers flexible options.** Ask your prospective partner if you can run both manual and automatic backups. Will your partner allow you to test the restoration feature to an alternate folder so you can have peace of mind that it actually works?





- **Has a good track record of great customer service.** Are they accessible 24/7? Do they have dedicated staff who can answer your questions quickly and knowledgeably? Do they have access to the latest product support information to meet your needs?
- **Can ensure the privacy of your data.** Demand a privacy policy and information that clearly spells out their backup procedures. Check to ensure they won't share your name, contact information or files with any third parties.
- **Offers a user interface that's easy to use.** The last thing you want when attempting to restore data is to try to figure out how to use the program. Become familiar with the program. Give your provider feedback when you can't easily find the answers to your questions. This helps them improve their Knowledge Base and Help files. Make sure your provider has support methods that fit your specific needs. Get to know the program well, so you can navigate it quickly and easily when you need to.

“ACS Technologies has nearly three decades of experience providing churches and other ministries with trustworthy software solutions that meet their specific needs.”

► Keep It Simple

Churches are adapting to the demands of today's growing information handling requirements by choosing data security solutions that help them simplify – not complicate – their efforts. While tapes, CDs, and DVDs can keep the task of backing up data “under tighter control” because it is administered by one person at your church, the ongoing administration and maintenance of the system can become cumbersome.

The responsibility of data security can also become “one person's job,” which makes your ministry vulnerable. Adopting a ministry-wide data security strategy is the first step to ensure your data is kept safe. Another key is to instruct your staff to save their documents and files to specific places on the server – rather than to their desktop – to file locations that are backed up every night.

Consider how scheduled backups to remote servers over the Internet can ease administrative time and resources spent on performing data security manually. In the event of a virus attack, natural disaster or accidental keystroke, restoring your ministry's vital data can be done with the click of a mouse.

For more information about how ACS Technologies' LiveStor product can meet your data security needs, please visit lvestor.com or call 800-736-7425.



➔ More About ACS Technologies

ACS Technologies is a leading provider of information management solutions for churches, schools, and other faith-based organizations. Founded in 1978, ACS Technologies serves over 22,000 organizations worldwide. From church management software to forms and supplies to professional Web sites and consulting, we offer six product and service suites in order to meet our clients' varied needs.

Since 1978, ACS Technologies has developed outstanding software products designed specifically for faith-based organizations, focusing on the special needs you address every day. We've designed our products to work together, integrating them to increase efficiency and reduce redundancies for your benefit. Our mission is simple, and our vision is focused – we empower our client partners with specially designed software solutions

➔ Contact information

ACS Technologies
180 Dunbarton Drive
Florence, SC 29501

800.736.7425
solutions@acstechnologies.com
acstechnologies.com