Aardsma Archives *prepare well. protect well.*

Protect Church Members' Personal Information

IS YOUR MEMBERS' DATA PROTECTED?

Churches commonly collect and store members' personal information. You will find everything from mailing lists and donation records to Social Security numbers and payment card information in the average church database. Unsecured, this data could make church members vulnerable to criminals—putting ministries and church members at risk.

Carefully managing this information not only makes business sense, it can also reduce the likelihood of crippling data loss, embarrassing public disclosures, and lawsuits.

What You Can Do:

Improve physical security

These seven tips are excerpted from *Security & Privacy— Made Simpler*, a resource from the Better Business Bureau. To obtain a copy, visit www.bbb.org/securityandprivacy.

- **Shred papers** containing personally identifiable information before throwing them away.
- **Send and receive** business mail from a secured mailbox or post office box.
- **Verify a church member's identity** before providing any personal or financial information by telephone or e-mail.
- **Secure your building** with locks and alarms.
- **Store** business, employee, and membership records in locked cabinets.
- **Limit** staff and volunteer access to sensitive information.
- **Train** office workers how to protect the privacy, confidentiality, and security of personal information.

(Continue page 2)

What You Can Do:

Improve Computer Security

- **Hire an expert.** Find an established computer support company that has a good reputation, stands behind its work, and comes highly recommended by other clients.
- **Patch your operating system.** This is your first line of defense, and it's free. Software companies regularly issue free updates to close holes hackers could climb through. Download them as soon as you learn that they're available.
- **Own virus and spyware protection.** This protection is essential, even for a one-computer office.
- **Update virus definitions daily.** Most software can be programmed to update virus definitions automatically. If your computer hasn't updated its virus definitions in several days (or weeks), your subscription may have expired. Contact your software manufacturer.
- **Scan computers weekly for malicious software.** Most virus and spyware protection software can be programmed to do this automatically.
- **Install a dependable firewall.** Both hardware and software firewalls are designed to prevent unauthorized access to a network. Hardware firewalls tend to work best.
- **Secure your wireless network.** Use encryption to translate information into a secret code that computers can decipher only with the correct password. Otherwise, you're inviting anyone with a wireless laptop to access church computers.
- **Preserve critical Data.** Back up business records daily, weekly, or monthly, depending on the size of your church. Store backups in a secure, off-site location, such as a safe-deposit box. This protects your ministry from losing records to computer breaches and other events, such as tornadoes, floods, or fires.
- **Limit access with passwords.** Use passwords to limit employee and volunteer access to sensitive information. Train office workers to keep passwords private.
- **Change passwords frequently.** Be sure to issue new passwords when an employee or volunteer stops working in the office and no longer needs to view ministry records.

(Continue page 3)

Cyber Insurance available

Computer-related liability coverage is available. Among other scenarios, this coverage applies to claims arising out of the ministry organization's inadvertent failure to protect personal information that is stored electronically, such as access passwords, bank account numbers, credit card numbers, or Social Security numbers. This specialized endorsement will fund covered damages that your ministry is ordered to pay because a computer-use error caused a member, client, or other outside party to suffer property damage, personal injury, or financial injury.

Protect Church Members' Personal Information

Resources

Here's where to turn for more information about identity theft prevention and personal information privacy.

The Federal Trade Commission:
http://www.ftc.gov/bcp/edu/microsites/idtheft/business/ index.html
http://www.ftc.gov/privacy/index.html

Privacy Rights Clearinghouse: https://www.privacyrights.org/identity.html

Identity Theft Resource Center: http://https://www.idtheftcenter.org/

The Better Business Bureau: https://www.bbb.org/

We would like to thank our corporate partner, Brotherhood Mutual, for being a valuable resource for this article.