Brotherhood Mutual
Insurance Company

Ministry Finances Checklist
Part 1: General Controls & Data Security

Financial crimes against churches and not-for-profit ministries are common. We have created this General Controls & Data Security checklist to help you strengthen financial accountability within your ministry. Consider reviewing this checklist at least once a year to determine whether your practices need further revision. Once you note areas needing improvement, develop a corrective-action plan and follow up periodically on corrective action measures.

General Financial Controls

- ▢ Do you have a comprehensive written policy governing the handling of your ministry's finances? Your policy should clearly spell out procedures for:
  - ▢ Handling cash
  - ▢ Making deposits and withdrawals
  - ▢ Documenting financial transactions
  - ▢ Reconciling bank statements
  - ▢ Accessing financial records
  - ▢ Providing oversight and accountability
  - ▢ Reporting suspicious incidents
- ▢ Do you conduct background checks on all employees and volunteers who deal with money? Companies that perform background checks typically offer special options for screening people with fiduciary responsibilities. Avoid selecting candidates who are undergoing a financial crisis or who have a history of theft.
- ▢ Do you divide control over financial operations among different people (i.e. the receipt, deposit, distribution, and documentation of money)?
- ▢ Do you conduct annual audits by someone other than your church's financial secretary or treasurer?
- ▢ Do you have an independent board or committee that understands the ministry's financial health and meets regularly to review monthly financial reports and the annual audit?
- ▢ Does your policy make it easy for employees or volunteers to report suspicions about fraud or embezzlement? Making it easy and safe for people to report suspicious financial activity will make it more likely that they'll come forward with helpful information.

Guidelines for Computerized Financial Records

- □ Do you back up vital business data regularly?
- □ Do you protect important programs from erasure?
- □ Do you store backups in a secure offsite location, such as a safe deposit box?
- □ Do you limit access to financial records with passwords?
- □ Do you change passwords frequently?
- □ Do you update your operating system regularly?
- □ Do you own current virus and spyware protection?
- □ Does a firewall protect your computer network from unauthorized users?
- □ Do you encrypt any payment card information stored on church computers?
- □ Do you have a disaster recovery plan? Do you regularly review and update it?