



KINGSWORTH

Division of First Southern National Bank

Year-End Church Financial Protection Checklist

A Practical Review for Stronger Stewardship in 2027



As you prepare for a new year of ministry, use this checklist to review your church's financial processes, identify potential gaps, and determine where a few simple changes could provide greater protection to your daily operations and for your staff.

ACCOUNT ACCESS & SECURITY

Review who has access to online banking	☐
Remove former staff, volunteers, or board members who no longer need access	☐
Review who can send payments or transfer funds	☐
Confirm transaction and payment limits are appropriate	☐
Verify contact information used for security verification	☐
Enable multifactor authentication wherever available	☐

PAYMENTS AND VENDORS

Require a second person to review large payments before they are sent	☐
Verify new vendors before making payments	☐
Confirm changes to payment instructions by calling a previously verified contact	☐
Avoid allowing the same person to both create and approve payments	☐
Review recurring payments and subscriptions	☐
Confirm who has authority to open accounts or credit cards on behalf of the church	☐

FINANCIAL ACCOUNTABILITY

Review who receives, records, approves, deposits, and reconciles church funds	☐
Use at least two people to count and deposit offerings	☐
Reconcile bank accounts each month	☐
Have someone other than the person issuing checks review account activity	☐
Provide regular financial reports to church leadership	☐
Schedule an annual financial review or periodic spot checks	☐

CHURCH CARDS & REIMBURSEMENTS

Review all active debit and credit cards	☐
Confirm cardholders and spending limits are still appropriate	☐
Require receipts for purchases and reimbursements	☐
Ensure no one approves their own expenses	☐
Review card statements regularly	☐
Close unused cards and accounts	☐

CYBERSECURITY & PREPAREDNESS

Keep software and devices updated	☐
Use strong, unique passwords and a password manager when possible	☐
Enable multifactor authentication on systems containing financial or sensitive information	☐
Back up important church data	☐
Review who has access to sensitive church, member, donor, and financial information	☐
Keep guest Wi-Fi separate from church administration systems	☐
Talk with staff about appropriate AI use and what church information should not be entered into public or personal AI accounts	☐
Establish which AI tools are approved for church use and review their privacy and data protections	☐
Document who to contact and what steps to take if a critical system becomes unavailable or compromised	☐

HAVE A QUESTION?

Every church's processes look a little different. If you'd like to talk through a question that came up during your review, we're happy to serve as a resource.

CONNECT WITH A RELATIONSHIP MANAGER

STAFF & CONGREGATION AWARENESS

Train staff to recognize suspicious emails, texts, and phone calls	☐
Establish a process for verifying urgent financial requests	☐
Encourage staff to pause and verify unexpected payment requests	☐
Remind members that church leaders will not unexpectedly request gift cards by text or email	☐
Review access to church directories and personal information	☐
Establish a clear, confidential way for staff or members to report concerns	☐