INSURANCE READINESS · FAMILYSENTINEL.ORG

The 12-Control Insurance-Readiness Checklist

This is the self-check version of the standard cyber-insurers now ask small organizations about. Work through the 12 controls below in order. Check the box only if you can honestly answer yes today — not "we plan to." Use the notes line under each one to jot down evidence — a screenshot, a policy date, a report — so it is ready when your broker or insurer asks. Most organizations complete this in about 20 minutes.

☐ 1 **MFA on every email account**

Every staff and volunteer email account requires a second step to sign in — a code or approval on a phone — not just a password.

Notes / evidence:

☐ 2 **MFA on admin and remote access**

The admin console and any remote-access path (VPN, remote desktop) also require MFA — not just regular mailboxes.

Notes / evidence:

☐ 3 **Privileged accounts separated and reviewed**

Day-to-day email users don't also hold admin rights on their everyday account; admin access lives on a separate, reviewed account.

Notes / evidence:

☐ 4 **Email authentication enforced (SPF, DKIM, DMARC at reject)**

Your domain publishes authentication rules and instructs receiving mail systems to reject anything that fails — not just flag it.

Notes / evidence:

☐ 5 **Email filtering with human-verified alerting**

A person actually reviews messages flagged as possible targeted fraud — not just an automated rule that silently deletes them.

Notes / evidence:

☐ 6 **Encrypted, offline-capable backups — actually tested**

Data is backed up somewhere an attacker with access to your live systems can't also delete, and a restore has been tested and confirmed to work.

Notes / evidence:

☐ 7 **Endpoint protection (EDR) on staff computers**

Computers used for organization business run active protection software that can detect and stop malicious activity, not just default antivirus.

Notes / evidence:

☐ 8 **Written incident-response plan with named roles**

A short document says who calls the bank, who calls the insurer, and who communicates with the congregation or members if something goes wrong.

Notes / evidence:

☐ 9 **Annual security-awareness training + a phishing exercise**

Staff and key volunteers receive scam-awareness training at least once a year and have completed at least one practice phishing exercise.

Notes / evidence:

☐ 10 **Access reviews at least quarterly**

Someone periodically checks who can touch money, sensitive data, and the admin console, and removes access no longer needed.

Notes / evidence:

☐ 11 **Vendor / payout-change verification procedure**

Before acting on any bank-detail change for a vendor or payee, someone calls a known phone number to confirm it — never a number from the request itself.

Notes / evidence:

☐ 12 **Known-exploited-vulnerability & breach-exposure watch**

Something or someone is watching whether your domain, email addresses, or public-facing services appear in breach data or carry actively-exploited vulnerabilities.

Notes / evidence:

Scoring key

12 / 12

Renewal-ready. Keep your evidence organized for next renewal.

9–11

A few documented gaps — normal at this stage.

Under 9

Expect broker questions. Start with MFA and tested backups.

Bring this to your broker

Take this completed worksheet — boxes checked, evidence notes filled in — to your insurance broker or renewal conversation. It is written in the same terms most cyber-insurance applications use, so it doubles as a plain-language answer key. It supports eligibility, underwriting readiness, and risk reduction; it does not guarantee premiums, coverage, claim payment, or insurer approval — those decisions remain with your insurer and broker.

FamilySentinel.org · (940) 281-6672 · security@familysentinel.org

---

About this checklist: prepared by Family Sentinel, a Texas-based service that helps churches, nonprofits, and small organizations monitor email for fraud and prepare the evidence insurers and brokers ask for at renewal. Learn more at **FamilySentinel.org**.