Squared Away Tech: Vendor Security Answers

Pre-filled answers for your vendor file or written information security plan (WISP). Last reviewed November 26, 2026. Current version: www.squaredawaytechfl.com/trust/

Why you may need this

The FTC Safeguards Rule, 16 CFR 314.4(f), requires covered financial institutions, including tax preparers, to (1) take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for customer information, (2) require those safeguards by contract, and (3) periodically assess service providers based on the risk they present. These answers are offered to help with steps 1 and 3; the signed service agreement covers step 2. This document is general information, not legal advice, and your own risk assessment decides whether it is enough.

1. Vendor details

Legal name	Squared Away Tech LLC, a Florida limited liability company (veteran-owned)
Mailing address	11161 E State Rd 70, Unit 110-1547, Lakewood Ranch, FL 34202
Security contact	Greg Mitchell, Managing Member. greg@squaredawaytechfl.com, (941) 479-1075. Security reports: www.squaredawaytechfl.com/.well-known/security.txt
Services	Microsoft 365 security reviews, hardening, device management and administration for small offices, delivered remotely
Credentials	Microsoft Certified: Windows Server Hybrid Administrator Associate. Member, Microsoft AI Cloud Partner Program.

2. Access to your systems

How is access granted?	Your admin creates a named account for Squared Away Tech in your own Microsoft 365 tenant (for example, squaredaway-admin@yourdomain). You can see, disable or delete it at any time. No shared logins.
Least privilege?	Yes. The Security Checkup uses look-only roles (Global Reader, plus View-Only Organization Management for Exchange if needed) and cannot change settings. Change rights are granted only for work you approve, limited to that work.
Time-limited?	Yes. The written authorization lists a start date and an end date.
MFA on vendor access?	Yes. Multi-factor authentication is registered on the vendor account, on the vendor's own device, before first use.
Partner delegated access (GDAP)?	Not used at this time. Access is only through the named account in your tenant.
Change control	No change is made without written approval (email is fine) from the owner or an officer. Each project ends with a change log.
Removal at the end	The vendor account is deleted (and the one-time consent for Microsoft's look-only tool can be removed) when the work ends. Removal is confirmed in writing.

3. Passwords and credentials

Does the vendor see our passwords?	No. Your admin enters their own password on their own device.
Does the vendor keep our credentials?	No. Emergency (break-glass) admin passwords and sign-in keys created during a project are kept by the owner (sealed envelope or the owner's password manager). Squared Away Tech does not keep a copy.

4. Your data: what, where, how long

What is collected?	Settings and reports only: user and admin lists, sign-in and MFA settings, mail-flow and forwarding settings, device status. Email content and files are not opened during a Checkup.
Where is it stored?	Scan results, exports and screenshots are kept only on the vendor's computer, which is protected with BitLocker full-disk encryption. Never in personal email, personal cloud storage or on USB drives. Files are shared with you by expiring link on request.

Retention	Scan results: deleted within 30 days of the report, or when follow-up work you hire us for is done. Final report, signed approval and invoice: kept for the relationship plus 3 years as business records, then deleted. Earlier deletion on request.
Sharing	Your information is not shared with anyone unless you ask (for example, with your IT person) or the law requires it.
Contract terms	A signed service agreement is required before any work. Its confidentiality section covers access only as needed, no copies kept longer than needed, return or deletion at the end, and access removal confirmed in writing. Healthcare clients: a business associate agreement (BAA) is signed before access.

5. The vendor's own security

Email authentication (squaredawaytechfl.com)	SPF published; DKIM signing keys published for Microsoft 365; DMARC at p=quarantine, 100% of mail, with reporting; MTA-STS published and set to enforce, naming only Microsoft 365 mail servers; TLS reporting on. Checked November 26, 2026 in public DNS; you can verify these yourself.
Vendor admin accounts	The business email account greg@squaredawaytechfl.com uses multi-factor authentication (MFA). The emergency admin account for Squared Away Tech's own Microsoft 365 signs in with a passkey (phishing-resistant). Client-tenant accounts use MFA as described above.
Vulnerability reporting	security.txt published at www.squaredawaytechfl.com/.well-known/security.txt

Questions not covered here? Email greg@squaredawaytechfl.com and I will answer in writing for your file. Prepared by Greg Mitchell, Managing Member, Squared Away Tech LLC.

Reviewed by (your office): _____ Date: _____ Next review: _____