JPert INC
Managed IT & Cybersecurity · Northern Virginia

WHITE PAPER · WEALTH MANAGEMENT

Wealth Management IT Setup Guide: Reg S-P and FINRA

How small registered investment advisers, broker-dealers and other wealth managers should set up IT to protect client accounts and meet the rules now in force. Each step says plainly whether a rule **requires** it or official guidance **recommends** it.

By Umair Akhtar, Founder & President, JPert INC
Published November 1, 2026
Last reviewed November 1, 2026
About a 13-minute read

JPert INC
1934 Old Gallows Road, Suite 360, Vienna, VA 22182
703-576-8200 · jpert.com
Free to share. The latest version is always at https://jpert.com/white-papers/wealth-management-it-setup

Scan for the latest version

The short version

- The SEC's amended Regulation S-P is now in force for every firm size: larger entities had to comply by December 3, 2025 and smaller entities by June 3, 2026.
- It requires a written incident response program, notice to affected customers no later than 30 days after you learn of unauthorized access to sensitive information, and service providers that notify you within 72 hours of a breach.
- The SEC's 2022 proposal for a separate adviser cybersecurity rule was withdrawn in June 2025. Do not plan around it.
- Advisers that are not registered with the SEC, and tax practices, fall under the FTC Safeguards Rule instead, which has its own list of required controls and a 30-day FTC notice for breaches affecting 500 or more people.

Who this is for and how to read it

This white paper is for principals, chief compliance officers and operations leads at RIAs, broker-dealers and family offices with roughly 5 to 100 people. Every recommendation is labeled:

- **REQUIRED** A rule requires it today.
- **RECOMMENDED** Official guidance from the SEC, FINRA, NIST or CISA recommends it.

Which rules apply depends on how your firm is registered. This is general guidance, not legal or compliance advice; confirm your obligations with your compliance consultant or counsel.

The rules that apply today

Amended Regulation S-P (SEC-registered firms)

REQUIRED The SEC amended Regulation S-P in 2024 (published June 3, 2024; effective August 2, 2024). It covers broker-dealers, investment companies, registered investment advisers and transfer agents. Compliance was required by December 3, 2025 for larger entities and June 3, 2026 for smaller entities, so every covered firm should now be compliant. The amendments require:

- A written **incident response program** reasonably designed to detect, respond to and recover from unauthorized access to or use of customer information.
- **Notice to affected individuals** as soon as practicable, but not later than **30 days** after becoming aware that sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.
- Written **oversight of service providers**, including a requirement that they notify the firm **within 72 hours** of a breach affecting customer information.
- Written records showing compliance.

The SEC's size categories do not match FINRA's, so check the definitions in the adopting release if you are unsure which date applied to you.

What was proposed and withdrawn

The SEC proposed a separate cybersecurity risk management rule for advisers and funds in February 2022. It was formally withdrawn in June 2025, along with a broker-dealer cybersecurity proposal and an adviser outsourcing proposal. Any material that still describes those proposals as coming rules is out of date.

Other rules that touch IT

- REQUIRED **Regulation S-ID** requires covered firms to have a written identity theft red flags program.
- REQUIRED Advisers must have written compliance policies under the **compliance program rule** (Rule 206(4)-7), which in practice includes cybersecurity and data

protection.

- REQUIRED Broker-dealers have FINRA's supervision rule (**Rule 3110**) and business continuity rule (**Rule 4370**).

Firms under the FTC Safeguards Rule

REQUIRED Investment advisers not required to register with the SEC, and tax preparers, are covered by the FTC Safeguards Rule (16 CFR Part 314). It requires a "Qualified Individual" to run the program, a written risk assessment, specific safeguards including MFA, encryption, an inventory and secure disposal, regular testing, staff training, service provider oversight, a written incident response plan and an annual report to the board. Since May 2024 it also requires notice to the FTC within 30 days of discovering a breach of unencrypted information on 500 or more consumers. Firms with information on fewer than 5,000 consumers are exempt from some of the written-document and testing requirements. Separately, the IRS reminded tax professionals in August 2026 that federal law requires them to keep a Written Information Security Plan.

Virginia's breach law

REQUIRED Virginia's breach law (Va. Code 18.2-186.6) also applies to Virginia residents' personal information. It includes provisions for firms that follow their primary regulator's notice rules; ask counsel how it applies to you.

Step 1: Accounts, passwords and multi-factor sign-in

- RECOMMENDED **Multi-factor sign-in (MFA) on email, remote access, cloud apps and every admin account.** CISA's ransomware guide asks for phishing-resistant MFA on all services, starting with email and remote access. Prefer an authenticator app, passkey or security key over text messages.
- RECOMMENDED **Long passphrases and a password manager.** Current NIST guidance (SP 800-63B, Revision 4) says passwords used alone should be at least 15 characters, should be checked against lists of leaked passwords, and should not be forced to change on a schedule unless there is a sign they were stolen.

- RECOMMENDED **One login per person and separate admin accounts.** Day-to-day work happens on standard accounts. Only a few people hold administrator rights, on separate logins.
- RECOMMENDED **Access ends on the last day.** When someone leaves, turn off email, remote access, shared passwords and building access the same day.

FINRA's 2026 Annual Regulatory Oversight Report lists MFA for staff, contractors and customers among the effective practices it has seen. Pay special attention to custodian and trading platform logins, which should have MFA and be limited to the people who need them.

Step 2: Email, account takeover and money movement

The FBI's 2025 Internet Crime Report recorded more than $3 billion in business email compromise losses. For a wealth manager, the classic attack is an email that appears to come from a client asking to move money.

- RECOMMENDED **Verify every money movement request by phone**, using a number already on file, before acting. FINRA lists verifying instructions before moving funds as an effective practice.
- RECOMMENDED **Watch for account takeover and lookalike domains.** FINRA's report highlights monitoring for imposter domains that mimic your firm.
- RECOMMENDED **Email authentication** (SPF, DKIM and DMARC) and outbound email scanning, both noted by the FTC and FINRA respectively.
- RECOMMENDED **Phishing training and tabletop exercises**, both on FINRA's list of effective practices.

Step 3: Computers, phones and personal devices

- RECOMMENDED **Encrypt every laptop and phone** that holds work data, so a lost device is a hardware problem, not a data breach. NIST's small-business guide calls for full-disk encryption on laptops and tablets.

- RECOMMENDED **Turn on automatic updates**, and patch internet-facing systems and anything on CISA's Known Exploited Vulnerabilities list first.
- RECOMMENDED **Replace unsupported systems.** Windows 10 support ended October 14, 2025. Machines that cannot upgrade yet need Microsoft's paid Extended Security Updates, which are only available for a limited time, and should be replaced.
- RECOMMENDED **Endpoint protection that someone actually watches**, on every computer. Alerts that nobody reviews do not stop an attack.

RECOMMENDED FINRA's report also points to a written policy for personal devices (BYOD). If advisers read client email on personal phones, require a passcode, encryption and the ability to remove firm data if the phone is lost or the adviser leaves.

Step 4: Network and Wi-Fi

- RECOMMENDED **Separate networks** for staff computers, guest Wi-Fi, and printers, cameras and other smart devices. CISA calls for network segmentation and a current diagram of how data moves.
- RECOMMENDED **WPA3 Wi-Fi** where your equipment supports it, with a long passphrase that changes when staff leave. Guests get internet access only.
- RECOMMENDED **No remote desktop open to the internet.** CISA says remote desktop should never be exposed directly. Use a VPN or secure remote-access service with MFA.
- RECOMMENDED **A supported business firewall**, kept updated and replaced when the manufacturer stops supporting it.

Network segmentation is also on FINRA's list of effective practices.

Step 5: Service providers under Reg S-P

REQUIRED Amended Regulation S-P requires written policies to oversee service providers, including making sure they notify you within 72 hours of a breach affecting

customer information. That covers your IT provider, CRM, financial planning and portfolio software, email, file storage and backup providers.

- Keep a list of every provider with access to customer information and what they can reach.
- Make sure each contract includes the 72-hour notice and cooperation with your incident response program.
- Review providers' security at onboarding and periodically. FINRA lists vendor risk monitoring as an effective practice.

RECOMMENDED In 2022, CISA, the NSA, the FBI and allied agencies published joint guidance for organizations that use a managed service provider (MSP). It says your contract should require MFA on every account the provider uses, least-privilege access, defined incident reporting, backup and incident-response duties, and prompt removal of the provider's access when the contract ends. Ask any IT provider, including us, to show you those terms in writing.

Step 6: Backups and business continuity

- RECOMMENDED **Offline, encrypted, tested backups.** CISA's guidance is to keep offline, encrypted backups of critical data and regularly test them. Many offices follow the "3-2-1" practice (three copies, two types of storage, one off-site) to meet it.
- RECOMMENDED **Back up cloud email and files too.** Cloud services keep your data running, but they are not a full backup plan on their own. Check what is covered and for how long.
- RECOMMENDED **Test a restore** on a schedule and write down how long it took.

REQUIRED Broker-dealers must keep a written business continuity plan under FINRA Rule 4370, and every firm needs to be able to serve clients if systems are down. Make sure the plan names the systems that come back first and how you will reach clients and custodians.

Step 7: Your incident response program

REQUIRED Under Reg S-P your incident response program must be written and designed to detect, respond to and recover from unauthorized access to customer information, and to decide whether customer notice is required within the 30-day limit.

- RECOMMENDED Name who leads the response, who calls the custodian, counsel and the cyber insurer, and who decides on notice.
- RECOMMENDED Keep a printed copy, and practice once a year with a short tabletop exercise.
- RECOMMENDED Use NIST's incident response guidance (SP 800-61, Revision 3, April 2025) as the reference model.
- RECOMMENDED Report fraud to the FBI at ic3.gov quickly; the FBI says its Recovery Asset Team froze about 58% of the money it tried to recover in 2025 (about $679 million).

One-page setup checklist

Area	What to have in place	Status today
Incident response program	Written, tested, with a 30-day customer notice decision process	REQUIRED (Reg S-P)
Service providers	Written oversight; 72-hour breach notice in contracts	REQUIRED (Reg S-P)
Identity theft	Written red flags program	REQUIRED (Reg S-ID)
Business continuity	Written plan (broker-dealers, FINRA Rule 4370)	REQUIRED
MFA	Staff, contractors, custodian and trading logins, admin accounts	RECOMMENDED
Money movement	Phone verification on a known number before any transfer	RECOMMENDED
Email	SPF, DKIM, DMARC; lookalike domain monitoring; outbound scanning	RECOMMENDED
Devices	Encrypted, updated, monitored; personal device policy	RECOMMENDED
Network	Segmented; no exposed remote desktop; supported firewall	RECOMMENDED
Backups	Offline or locked copy; cloud data included; restores tested	RECOMMENDED
FTC-covered firms	Qualified Individual, risk assessment, 30-day FTC notice for 500+	REQUIRED (Safeguards Rule)

How JPert can help

JPert is a managed IT and cybersecurity company in Vienna, Virginia, near Tysons. As your IT provider we are one of the service providers Reg S-P asks you to oversee, so we put breach notice and incident cooperation terms in writing. Read about IT for wealth management firms, or book a free IT assessment.

Related reading from our Chronicles: SEC Reg S-P compliance checklist, RIA data breach response plan and email security for wealth managers.

Sources

Every recommendation above comes from these official sources, checked on November 1, 2026:

- Federal Register: Regulation S-P amendments (89 FR 47688, June 3, 2024)
- SEC: Regulation S-P Small Entity Compliance Guide
- SEC press release 2024-58: Regulation S-P amendments adopted
- FINRA: Regulation S-P compliance date reminder (November 2025)
- SEC: Withdrawal of the proposed adviser cybersecurity risk management rule
- FINRA: 2026 Annual Regulatory Oversight Report, Cybersecurity
- FINRA: Small Firm Cybersecurity Checklist
- FINRA Rule 4370: Business Continuity Plans
- FTC: Safeguards Rule, what your business needs to know
- FTC Safeguards Rule, 16 CFR Part 314 (eCFR)
- IRS: Tax professionals need a Written Information Security Plan (August 2026)
- Va. Code 18.2-186.6 (breach of personal information notification)
- FBI: 2025 Internet Crime Report
- NIST SP 800-63B Rev. 4: Authentication and passwords
- CISA: #StopRansomware Guide

- CISA, NSA, FBI and allied agencies: Protecting against cyber threats to MSPs and their customers (AA22-131A)
- NIST SP 800-61 Rev. 3: Incident response recommendations (April 2025)
- Microsoft: Windows 10 end of support and Extended Security Updates

This white paper is general information about IT and security practices, not legal or compliance advice. Rules change; we review this paper when the SEC, FINRA or FTC changes them. See our editorial policy.

FAQ

Common questions from wealth managers

When did the amended Regulation S-P take effect?

The amendments took effect August 2, 2024. Larger entities had to comply by December 3, 2025 and smaller entities by June 3, 2026, so all covered firms should now be compliant.

What does amended Regulation S-P require?

A written incident response program, notice to affected individuals no later than 30 days after the firm becomes aware of unauthorized access to sensitive customer information, written oversight of service providers including 72-hour breach notice from them, and records showing compliance.

Is the SEC's cybersecurity rule for advisers still coming?

No. The SEC proposed a cybersecurity risk management rule for advisers and funds in February 2022 and formally withdrew it in June 2025. Regulation S-P and the other existing rules still apply.

Which rule applies to advisers not registered with the SEC?

Investment advisers not required to register with the SEC are covered by the FTC Safeguards Rule, which requires a Qualified Individual, a written risk assessment, controls such as MFA and encryption, and notice to the FTC within 30 days of a breach affecting 500 or more consumers.

Want us to check your setup against this guide? Book a free IT assessment with our Vienna, VA team at jpert.com/contact or call 703-576-8200. We will give you a plain-English list of what to fix first.