

FREE PDF GUIDE

Cybersecurity and Privacy Rules for Texas RIAs

SEC, Reg S-P and Texas rules explained

October 2026

24unet.com

Denver (303) 468-5515 | College Station (979) 256-5100 | sales@24unet.com

Cybersecurity and Privacy Rules for Texas RIAs: SEC, TSSB and Texas Law

A 24uNet guide for Texas registered investment advisers

If you run a registered investment adviser in Texas, your cybersecurity duties come from three places. The first is a federal rule that depends on how you are registered. The second is the Texas State Securities Board (TSSB). The third is Texas breach law, which applies to every business. This guide explains what each one asks of you and how IT supports it.

> **Not legal advice.** This guide is general information about rules as of October 2026. How they apply depends on your firm, so confirm your obligations with your counsel.

Texas deadlines at a glance

Trigger	Who notifies whom	Deadline	Rule
Vendor learns of a breach of a customer information system	Vendor to SEC-registered adviser	No later than 72 hours	Reg S-P
Sensitive customer information accessed	SEC-registered adviser to individuals	No later than 30 days	Reg S-P
Unencrypted information of 500+ consumers acquired	State-registered adviser to FTC	No later than 30 days	FTC Safeguards Rule
Another breach notice is required and Texas clients may be affected	Texas-registered adviser to Securities Commissioner	At the same time	7 TAC 116.23
Breach of sensitive personal information	Any business to affected Texans	No later than 60 days	Bus. & Com. Code 521.053
250 or more Texans affected	Any business to Texas Attorney General	No later than 30 days	521.053
Vendor holds data it doesn't own	Vendor to data owner	Immediately	521.053

Federal rules: it starts with how you are registered

The first question for any adviser is where you are registered. SEC-registered advisers fall under Regulation S-P. State-registered advisers generally fall under the FTC Safeguards Rule instead. Both groups also answer to their state's securities rules and breach law.

SEC-registered advisers: Regulation S-P

The SEC amended Regulation S-P in May 2024. Larger firms had to meet the new requirements by December 3, 2025, and smaller firms by **June 3, 2026**. Both dates have passed, so the amended rule now applies to every SEC-registered adviser. It requires:

- **An incident response program.** You need written procedures to detect, respond to and recover from unauthorized access to customer information.
- **Service-provider oversight with a 72-hour notice.** You must oversee vendors so they protect customer information and notify you as soon as possible, and no later than **72 hours** after they learn of a breach of a customer information system. The rule doesn't require specific contract wording. Written contract terms are the usual way to show this oversight.
- **Customer notice within 30 days.** Affected individuals must be notified as soon as practicable, and no later than **30 days** after you become aware of unauthorized access to sensitive customer information. A reasonable investigation may show that substantial harm is not likely, but you have to document it.
- **Disposal and records.** The rule expands disposal duties and requires written records of all of the above.

Source: SEC final rule, Release 34-100155

How 24uNet helps: We write and test incident response plans and provide incident response support when something happens. Our 24/7 managed detection and response has security analysts reviewing alerts around the clock. We also review the 72-hour notice language in your IT and vendor contracts, so your oversight is on paper as well as in practice.

Regulation S-ID: identity theft red flags

SEC-registered firms with covered accounts must also keep a written identity theft prevention program. The program must spot and respond to red flags and be updated over time. A 2025 SEC settlement faulted a program that left out

cybersecurity red flags after email accounts were taken over. Source: 17 CFR Part 248, Subpart C; SEC order 34-104255

How 24uNet helps: Our identity threat detection and response watches Microsoft 365 for account takeover and responds when it happens. We also set up phishing-resistant login and multifactor authentication, so a stolen password is not enough.

State-registered advisers: the FTC Safeguards Rule

State-registered advisers are generally outside Reg S-P and fall under the FTC Safeguards Rule. The rule calls for a written information security program led by a qualified individual. It also requires risk assessments, safeguards such as multifactor authentication and encryption, and vendor oversight. Since May 13, 2024, you must notify the FTC within 30 days of discovering that unencrypted information of 500 or more consumers was acquired without authorization. Source: FTC: What your business needs to know; Federal Register, Nov 13, 2023

How 24uNet helps: Our security assessments, the Security Baseline and annual external vulnerability scans give you the risk assessment and written findings this rule calls for. Security awareness and phishing training covers the people side.

Texas rules for investment advisers

TSSB Rule 7 TAC 116.23: telling the Securities Commissioner

Since February 27, 2020, a Texas-registered investment adviser has had to notify the Texas Securities Commissioner when a cybersecurity incident requires notice to a government agency, law enforcement, a self-regulatory organization or customers. That applies when Texas clients may be affected. The notice goes out **at the same time** as the other notices. A copy of the notice you're already sending satisfies the rule. Include the number of affected Texas clients if you know it. Source: 7 TAC 116.23

In practice, this is one easy line to miss in an incident plan. Add a step that says "copy the TSSB and count Texas clients."

How 24uNet helps: Our incident response planning builds the TSSB step into your plan. If an incident happens, our incident response support helps you collect what the notice needs.

TSSB cybersecurity guidance

The TSSB also publishes voluntary guidance for securities professionals. It covers risk assessment, encryption, secure email, backups and due diligence on cloud vendors. This guidance is not a rule, but it shows what the regulator expects good practice to look like. Source: TSSB: Are You Secure?

The TSSB's broader rules in 7 TAC Chapter 116 also govern books, records and written policies. Treat incident and vendor records as part of your required files.

How 24uNet helps: We set up Microsoft 365 email encryption and handle your backup and disaster recovery and business continuity with tested restores. We also keep the vendor and incident records examiners ask for.

Texas breach law: Business & Commerce Code 521.053

Texas breach law applies to every business that holds Texans' sensitive personal information, however the firm is registered.

- **Individuals:** notify without unreasonable delay, and no later than **60 days** after determining a breach occurred.
- **Texas Attorney General:** if **250 or more Texans** are affected, notify as soon as practicable and no later than **30 days**, using the Attorney General's online form.
- **Vendors:** a vendor that maintains data it doesn't own must notify the owner **immediately** after discovering a breach.

Sources: Bus. & Com. Code 521.053; Texas AG data breach reporting

An SEC-registered adviser may therefore face two clocks: 30 days under Reg S-P and 60 days under Texas law. Plan to the shorter one.

How 24uNet helps: We build a breach runbook that tracks every clock, including the Attorney General's online form. We also help you add notice terms for vendors that hold your data.

Does the Texas Data Privacy and Security Act apply?

For most advisers, likely not. The TDPSA exempts financial institutions subject to Title V of the Gramm-Leach-Bliley Act. It also exempts small businesses as defined by the SBA, except for its rule on selling sensitive data. Texas breach law still applies either way. Sources: HB 4 enrolled text; Texas AG: TDPSA

How 24uNet helps: A security assessment maps where personal data lives, so you know what a breach would touch.

Checklist: how IT supports each rule

Rule	What it asks	How IT supports it
Reg S-P incident response	A written program that works	Written plan tested with tabletop exercises; 24/7 managed detection and response with analysts reviewing alerts; Microsoft 365 audit logs kept long enough to investigate
Reg S-P vendor notice	Oversight of service providers	Vendor and data inventory; IT agreement terms for notice within 72 hours, evidence preservation and cooperation
Reg S-P customer notice	Knowing what was accessed	Logging that shows which mailboxes and files were touched; a written record of each decision
Reg S-P disposal	Secure disposal	Device wipe through Intune; data-return and destruction terms
Reg S-ID	A red flags program	Detection of email account takeovers; multifactor authentication and Conditional Access in Microsoft 365; call-back checks before moving money
FTC Safeguards Rule	A written security program	Annual risk assessment; multifactor authentication; encryption; security awareness training; vendor reviews
7 TAC 116.23	Notice to the Commissioner	Incident plan step to copy the TSSB and count Texas clients
TSSB guidance	Secure email, encryption, backups	Microsoft 365 email encryption; backups with tested restores; cloud vendor due diligence
Texas 521.053	Notice to individuals and the AG	Breach runbook with the AG online-form step; vendor terms for immediate notice

How a Texas RIA should respond to a cyber incident

1. Contain the incident and preserve evidence.
2. Work out what customer and personal information was accessed.
3. Notify affected individuals: within 30 days under Reg S-P if you are SEC-registered, and within 60 days under Texas law.
4. Notify the Texas Attorney General within 30 days if 250 or more Texans are affected.
5. If you are Texas-registered, copy the Securities Commissioner at the same time.
6. Document every decision and update your plan.

How 24uNet supports advisers

- **24/7 managed detection and response:** security analysts review alerts day and night.
- **Incident response planning and support:** written plans, tabletop tests, and hands-on help when an incident hits.
- **Vendor and service-provider oversight:** we review the 72-hour notice language in IT contracts and build vendor inventories.
- **Microsoft 365 security hardening and identity threat detection and response:** account takeover detection and response.
- **Phishing-resistant login and multifactor authentication.**
- **Backup, disaster recovery and business continuity.**
- **Security assessments,** the Security Baseline, and annual external vulnerability scans.
- **Security awareness and phishing training.**
- **Managed IT,** including bundled IT and security in our Cybersecurity Business Bundle.
- **Lone Star Assurance:** our Texas cybersecurity program for Texas firms.

Talk to 24uNet. Denver (303) 468-5515 · College Station (979) 256-5100 · sales@24unet.com · 24unet.com