



**FREE PDF GUIDE**

# Cybersecurity and Privacy Rules for Colorado RIAs

SEC, Reg S-P and Colorado rules explained

October 2026

---

**24unet.com**

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

# Cybersecurity and Privacy Rules for Colorado RIAs: SEC, Division of Securities and Colorado Law

## A 24uNet guide for Colorado registered investment advisers

If you run a registered investment adviser in Colorado, your cybersecurity duties come from three places. The first is a federal rule that depends on how you are registered. The second is the Colorado Division of Securities. The third is Colorado breach law, which applies to every business. Colorado's AI law is also changing. This guide explains each one 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.

## Colorado 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 |
| Breach of personal information                             | Any business to affected Coloradans       | No later than 30 days     | C.R.S. 6-1-716      |
| 500 or more Coloradans affected                            | Any business to Colorado Attorney General | No later than 30 days     | 6-1-716             |
| Vendor discovers a breach                                  | Service provider to data owner            | Must notify and cooperate | 6-1-716             |

## 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.

## **Colorado rules for investment advisers**

### **Division of Securities Rule 51-4.14(IA): written cybersecurity procedures**

Colorado-registered advisers must keep written cybersecurity procedures suited to the firm. The procedures must cover:

- a risk assessment, repeated each year where reasonably possible
- employee training
- secure email, including encryption
- authentication of employees and of client instructions
- automatic device locking and reporting of lost devices
- vendor relationships
- telling clients about the risks of electronic communication

The rule now ties into the written-policies requirement in Rule 51-4.12(IA). Sources: [3 CCR 704-1, Rule 51-4.14\(IA\)](#); [Rule 51-4.12\(IA\)](#); [Division of Securities announcement](#)

**How 24uNet helps:** This rule reads like an IT checklist, and we cover it end to end. We provide annual security assessments, the [Security Baseline](#) and external vulnerability scans. We run security awareness and phishing training and set up Microsoft 365 email encryption. We add phishing-resistant login and multifactor authentication, Intune auto-lock and remote wipe, and call-back procedures to verify client instructions. Vendor reviews round it out.

### **Colorado breach law: C.R.S. 6-1-716**

Colorado breach law applies to every business that holds Coloradans' personal information.

- **Individuals:** notify no later than **30 days** after determining a breach occurred.
- **Colorado Attorney General:** if **500 or more Coloradans** are affected, notify no later than **30 days**, using the [Attorney General's online form](#).
- **Service providers:** must notify the business and cooperate.
- **Security and disposal:** Colorado also requires reasonable security procedures and written disposal policies (C.R.S. 6-1-713 and 6-1-713.5).

Sources: [C.R.S. 6-1-716](#); [Colorado AG: data protection laws](#)

Colorado's 30-day deadline for notifying individuals matches the 30 days in Reg S-P. That leaves little room to work out what happened.

**How 24uNet helps:** Our 24/7 managed detection and response, with analysts reviewing alerts, catches problems early. Our incident response support and Microsoft 365 logging help you see what was accessed. We also write your disposal policy and handle secure device wiping.

### Does the Colorado Privacy Act apply?

Generally not to advisers. The CPA does not apply to financial institutions subject to the Gramm-Leach-Bliley Act (C.R.S. 6-1-1304). It also applies only above consumer-data thresholds that most small firms don't reach. In October 2025 the Attorney General proposed amendments to the CPA rules, and we found no change to the GLBA exemption. Breach law still applies. Sources: [C.R.S. 6-1-1304](#); [Proposed CPA rule amendments](#)

### Colorado's AI law: what changes on January 1, 2027

- **SB 24-205**, the original Colorado AI Act, was delayed to June 30, 2026. A federal court has since stayed its enforcement (*xAI v. Weiser*, April 27, 2026).
- **SB 26-189**, signed May 14, 2026, repeals and replaces it. The new law sets notice-based rules for automated decision-making technology used in consequential decisions, including financial services. It takes effect **January 1, 2027**.
- For most advisers the impact is likely limited, unless they use automated tools to make decisions about financial services for consumers.

Sources: [Colorado AG: AI](#); [Colorado Legislative Council summary](#)

**How 24uNet helps:** Our Microsoft Copilot readiness work starts with an inventory of the AI tools your firm uses. We clean up permissions, review oversharing and set up sensitivity labels, so you know what AI can reach before the new law takes effect.

### How a Colorado RIA should respond to a cyber incident

1. Contain the incident and preserve evidence.
2. Work out what personal and customer information was accessed.
3. Notify affected Coloradans within 30 days, and follow Reg S-P if you are SEC-registered.
4. Notify the Colorado Attorney General within 30 days if 500 or more are affected.
5. Confirm notices from your vendors and get their cooperation.
6. Document every decision and update your procedures under Rule 51-4.14(IA).

### 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](#).
- **Microsoft Copilot readiness:** permissions cleanup, oversharing review and sensitivity labels.

**Talk to 24uNet.** Denver (303) 468-5515 · College Station (979) 256-5100 · [sales@24unet.com](mailto:sales@24unet.com) · [24unet.com](https://24unet.com)