REGULATION S-P

Cybersecurity Checklist

[Firm name] | Completed by [Name] | [Month DD, YYYY]

Before You Start

This checklist covers the cybersecurity side of Regulation S-P (17 CFR 248.30) as amended in 2024, for investment advisers registered with the SEC. It does not cover the privacy notice and opt-out parts of the regulation.

For each item, mark Yes, Partial or No, and write down where the proof is kept. A Yes with nothing in the evidence column should be treated as a No. An examiner can ask to see the document.

Compliance dates	December 3, 2025 for advisers with $1.5 billion or more in assets under management. June 3, 2026 for all other SEC-registered advisers.
Who it covers	SEC-registered investment advisers. Advisers not required to register with the SEC fall under the FTC Safeguards Rule (16 CFR Part 314) instead.
Rule text	ecfr.gov/current/title-17/section-248.30

1. Written Policies and Scope

Item	Rule	Evidence on file	Result
Written policies and procedures cover administrative, technical and physical safeguards for customer information	248.30(a)(1)	[Policy name, version, date]	☐ Yes ☐ Partial ☐ No
The policies are designed to keep customer information secure and confidential, protect against expected threats, and protect against unauthorized access or use that could cause substantial harm or inconvenience	248.30(a)(2)	[Policy section]	☐ Yes ☐ Partial ☐ No
A current list of the systems that hold customer information: CRM, custodian portals, planning software, email, file storage, backups	Supports (a)(1)	[System inventory, date]	☐ Yes ☐ Partial ☐ No
The firm knows which records are sensitive customer information, such as Social Security numbers, or account numbers and usernames with the passwords or codes that open them	248.30(d)(9)	[Data map or inventory column]	☐ Yes ☐ Partial ☐ No
The policies were reviewed in the firm's annual compliance review	Supports 206(4)-7(b)	[Annual review memo, date]	☐ Yes ☐ Partial ☐ No

2. Security Controls

The rule does not list specific controls. These are common controls firms use to show the safeguards in 248.30(a)(2) are working. If you do not use one, write down why and what you do instead.

Item	Rule	Evidence on file	Result
Multifactor authentication on email, the CRM, custodian portals and every admin account	Supports (a)(2)	[MFA report, date]	☐ Yes ☐ Partial ☐ No
Admin rights limited to the people who need them, and reviewed at least once a year	Supports (a)(2)	[Admin list, review date]	☐ Yes ☐ Partial ☐ No
Access removed on a person's last day, including vendor platforms and custodian logins	Supports (a)(2)	[Offboarding checklist]	☐ Yes ☐ Partial ☐ No
Laptops and phones that hold client data are encrypted and can be wiped remotely	Supports (a)(2)	[Device report, date]	☐ Yes ☐ Partial ☐ No
Operating systems and software are patched on a schedule, and every device runs endpoint protection	Supports (a)(2)	[Patch and device report]	☐ Yes ☐ Partial ☐ No
Email is set up with SPF, DKIM and DMARC, and DMARC is set to quarantine or reject	Supports (a)(2)	[DNS record check, date]	☐ Yes ☐ Partial ☐ No
Clients send and receive sensitive documents through a secure portal or encrypted email, not plain email	Supports (a)(2)	[Procedure or tool]	☐ Yes ☐ Partial ☐ No
Sign-in and admin activity logs are turned on and kept long enough to investigate an incident	Supports (a)(3)	[Log settings, retention]	☐ Yes ☐ Partial ☐ No
Backups of client data are tested by restoring a file at least once a year	Supports (a)(3)	[Restore test record, date]	☐ Yes ☐ Partial ☐ No
Staff complete security awareness training at least once a year	Supports (a)(2)	[Training records]	☐ Yes ☐ Partial ☐ No

3. Incident Response Program

Item	Rule	Evidence on file	Result
A written program to detect, respond to and recover from unauthorized access to or use of customer information, including customer notification procedures	248.30(a)(3)	[Plan name, version, date]	☐ Yes ☐ Partial ☐ No
Steps to assess the nature and scope of an incident and identify the systems and types of customer information involved	248.30(a)(3)(i)	[Plan section]	☐ Yes ☐ Partial ☐ No
Steps to contain and control the incident to stop further unauthorized access	248.30(a)(3)(ii)	[Plan section]	☐ Yes ☐ Partial ☐ No
Named people and an offline contact list: IT provider, counsel, cyber insurer, custodian	Supports (a)(3)	[Contact list, date]	☐ Yes ☐ Partial ☐ No
The plan was tested in the last 12 months, for example with a tabletop exercise, and the results were written down	Supports (a)(3)	[Exercise notes, date]	☐ Yes ☐ Partial ☐ No

4. Customer Notification

Item	Rule	Evidence on file	Result
A procedure for deciding whether notice is required, including a reasonable investigation of whether sensitive customer information has been, or is reasonably likely to be, used in a way that would cause substantial harm or inconvenience	248.30(a)(4)(i)	[Procedure section]	☐ Yes ☐ Partial ☐ No
If the firm cannot tell whose information was involved, notice goes to everyone whose sensitive customer information was in the affected system	248.30(a)(4)(ii)	[Procedure section]	☐ Yes ☐ Partial ☐ No
Notice goes out as soon as practicable, and no later than 30 days after the firm becomes aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred	248.30(a)(4)(iii)	[Procedure section]	☐ Yes ☐ Partial ☐ No
A notice template with every required item: what happened, the type of information, dates, how to contact the firm, a reminder to review account statements and report anything suspicious, fraud alerts, credit reports, and FTC identity theft guidance	248.30(a)(4)(iv)	[Template name]	☐ Yes ☐ Partial ☐ No

5. Service Providers

Item	Rule	Evidence on file	Result
Every vendor that receives, maintains, processes or can access customer information is on a vendor list. This generally includes the IT provider	248.30(d)(10)	[Vendor list, date]	☐ Yes ☐ Partial ☐ No
Written policies and procedures for vendor oversight, including due diligence and monitoring	248.30(a)(5)(i)	[Procedure section]	☐ Yes ☐ Partial ☐ No
Each vendor has a completed review on file, with the evidence it was based on (for example, a SOC 2 report)	Supports (a)(5)(i)	[Review form, date]	☐ Yes ☐ Partial ☐ No
The procedures are designed to make sure vendors take appropriate measures to protect customer information against unauthorized access or use	248.30(a)(5)(i)(A)	[Contract clause or attestation]	☐ Yes ☐ Partial ☐ No
The procedures are designed to make sure vendors notify the firm as soon as possible, and no later than 72 hours after becoming aware of a breach that gives someone unauthorized access to a customer information system the vendor maintains	248.30(a)(5)(i)(B)	[Contract clause or attestation]	☐ Yes ☐ Partial ☐ No
If a vendor will send customer notices for the firm, that is in a written agreement. The firm still owns the obligation	248.30(a)(5)(ii)-(iii)	[Agreement section, or N/A]	☐ Yes ☐ Partial ☐ No
Vendor reviews are repeated on a schedule, at least yearly for vendors that hold sensitive customer information	Supports (a)(5)(i)	[Next review dates]	☐ Yes ☐ Partial ☐ No

6. Disposal

Item	Rule	Evidence on file	Result
Written procedures for disposing of customer information and consumer information	248.30(b)(2)	[Policy section]	☐ Yes ☐ Partial ☐ No
Old devices are wiped or destroyed, paper is shredded, and vendors provide certificates of destruction	Supports (b)(1)	[Disposal log or certificates]	☐ Yes ☐ Partial ☐ No

7. Records You Can Produce

Rule 204-2(a)(25) lists the Regulation S-P records an adviser must keep. Rule 204-2(e)(1) says how long and where: at least five years from the end of the fiscal year of the last entry, in an easily accessible place, the first two in an appropriate office of the adviser.

Item	Rule	Evidence on file	Result
The written safeguards policies and procedures	204-2(a)(25)(i)	[File location]	☐ Yes ☐ Partial ☐ No
Records of any detected unauthorized access to or use of customer information, and the response and recovery	204-2(a)(25)(ii)	[Incident log location]	☐ Yes ☐ Partial ☐ No
Records of each investigation into whether notice was required, the basis for the decision, and a copy of any notice sent	204-2(a)(25)(iii)	[File location]	☐ Yes ☐ Partial ☐ No
The written service provider oversight policies and procedures	204-2(a)(25)(iv)	[File location]	☐ Yes ☐ Partial ☐ No
Any contract or agreement with a service provider under 248.30(a)(5)	204-2(a)(25)(v)	[File location]	☐ Yes ☐ Partial ☐ No
The written disposal policies and procedures	204-2(a)(25)(vi)	[File location]	☐ Yes ☐ Partial ☐ No
Someone other than the person who built the file can find each record above in a few minutes	Supports 204-2(e)(1)	[Name, date tested]	☐ Yes ☐ Partial ☐ No

8. Massachusetts Personal Information

Skip this section if the firm does not own or license personal information about Massachusetts residents.

Item	Rule	Evidence on file	Result
A written information security program (WISP) that meets 201 CMR 17.03	201 CMR 17.03	[WISP version, date]	☐ Yes ☐ Partial ☐ No
Contracts require service providers to maintain appropriate security measures for personal information	201 CMR 17.03(2)(f)	[Contract clauses]	☐ Yes ☐ Partial ☐ No

Summary

Section	Items	Yes	Partial	No
1. Written policies and scope	5			
2. Security controls	10			
3. Incident response program	5			
4. Customer notification	4			
5. Service providers	7			
6. Disposal	2			
7. Records you can produce	7			
8. Massachusetts personal information	2			
Total	42			

What to fix first. Every No or Partial needs an owner and a date. Start with sections 3, 4 and 5. The SEC's fiscal 2027 examination priorities say staff will evaluate response programs, customer notification procedures and oversight of service providers.

Completed by	[Name, title]
Reviewed by	[Chief Compliance Officer]
Date	[Month DD, YYYY]

ABOUT

About This Checklist

A cybersecurity checklist for SEC-registered investment advisers, built from the text of amended Regulation S-P and the books and records rule. Each item names the paragraph it comes from. Items marked "Supports" are controls the rule does not name but that firms use to show the required safeguards work.

How to use it

- Work through it with your CCO and your IT provider in the same room. Most items need both.
- Fill in the evidence column for every Yes. If you cannot point to a document, mark it Partial or No.
- For section 5, complete a Vendor Security Review for each service provider. The template is free at saberguard.tech/resources.
- Keep the completed checklist with your annual compliance review records.
- Run it again each year, and after any incident, new vendor, or system change.

Before you rely on it

This checklist reflects Regulation S-P as amended in May 2024 and the rule text on eCFR as of November 2026. It is not legal advice and it does not certify compliance. Confirm your firm's obligations with compliance counsel and adjust it to match your written policies and procedures.

Free to use

Use it, change it and share it inside your firm. If you would rather have the review done for you, or need help building the program behind it, contact SaberGuard.

Jonathan DeLeon, CISM, CCSP

SaberGuard, LLC | jonathan.deleon@saberguard.tech | saberguard.tech