Cybersecurity Baseline Checklist

A 10-minute self-check for small broker-dealers and RIAs

Firm name	
Date completed	
Completed by (names)	

How to use this checklist. This records what the Firm has in place on the date above. It is not a technical test of the Firm's systems. Check Y (yes), N (no), or DK (don't know). Every No or Don't know gets an owner and a target date in the last column, then list your top three gaps at the end.

#	Question	Y	N	DK	Notes, owner, and target date
A. Customer information					
1	We know every place customer information is kept (email, shared drives, CRM, vendor systems, and paper files).	☐	☐	☐	
2	Account forms and other client documents are moved out of email to a secure location once they are processed.	☐	☐	☐	
B. Vendors					
3	We have a list of the vendors that hold or can access customer information.	☐	☐	☐	
4	Each key vendor's contract requires it to tell us promptly if it has a breach. (Regulation S-P expects notice within 72 hours.)	☐	☐	☐	
C. Logins and access					
5	Multi-factor authentication (a code or app prompt in addition to a password) is on for everyone's email, e-signature, and client portal or file-sharing system.	☐	☐	☐	
6	Staff use a password manager or unique passwords for each system.	☐	☐	☐	
7	Every person has their own login. No shared accounts or passwords.	☐	☐	☐	
8	When someone leaves the Firm, their access is removed the same day.	☐	☐	☐	

© 2026 Compliance Matters NYC. You may use and share this checklist within your firm.

#	Question	Y	N	DK	Notes, owner, and target date
D. Devices and sending files					
9	Firm laptops are encrypted.	☐	☐	☐	
10	We send account forms and other sensitive client files securely, not as ordinary email attachments.	☐	☐	☐	
11	If staff use personal phones or computers for firm email, the Firm can remove firm data if a device is lost.	☐	☐	☐	
E. Money movement					
12	Any change to wire or payment instructions is confirmed by calling a phone number already on file, never a number in the request.	☐	☐	☐	
F. Training and reporting					
13	Staff had cybersecurity training in the past 12 months. Date: _____	☐	☐	☐	
14	Staff know who to tell if something looks suspicious, and that person is named in writing.	☐	☐	☐	
G. Backups and continuity					
15	Key data and systems are backed up, and backups are kept separate from the main systems.	☐	☐	☐	
16	A backup has been restored as a test in the past 12 months. Date: _____	☐	☐	☐	
17	Our BCP was reviewed in the past 12 months. Broker-dealers: our two FINRA emergency contacts are current.	☐	☐	☐	
H. Insurance					
18	We have cyber insurance, and the claims phone number is kept where we can reach it offline.	☐	☐	☐	

© 2026 Compliance Matters NYC. You may use and share this checklist within your firm.

#	Question	Y	N	DK	Notes, owner, and target date
I. Software updates					
19	Our IT provider and key vendors install security updates promptly, and we can confirm it when a major flaw is in the news.	☐	☐	☐	

Top gaps to address

#	Gap	Owner	Target date
1			
2			
3			

Answers reflect what the Firm knows on the date above. The Firm owns this checklist and decides how to address each gap. For general information only. Not legal advice or a complete cybersecurity program.

Reviewed and approved by (name and title)	
Signature	
Date	

© 2026 Compliance Matters NYC. You may use and share this checklist within your firm.