HINSHAW

Alerts

Are Your Cybersecurity Controls Ready for the New York State Department of Financial Services' Deadlines?

April 14, 2025
Privacy, Cyber & AI Decoded

In November 2023, New York State's Department of Financial Services (NYDFS) amended its cybersecurity regulation, Part 500. This legal alert provides an update for Covered Entities and Class A Businesses on the current NYDFS cybersecurity requirements for the remainder of the calendar year 2025.

NYDFS Upcoming Cybersecurity Requirements for 2025

- Certification of Material Compliance: **April 15**
- Technical Requirements: **May 1**
- Multi-factor Authentication (MFA) and Asset Inventory: **November 1**

What are the Annual Compliance Requirements?

On April 15, 2025, Annual Compliance submissions for the 2024 calendar year are due for "**Covered Entities**" and "**Class A Companies**" under New York's Department of Financial Services Amended Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500 (the "**Regulation**"). Organizations should be updating their Certification of Material Compliance from 2024.

The **Certification of Material Compliance** is a written statement that confirms the Covered Entity or Class A Business has substantially adhered to the applicable Regulation requirements for the previous calendar year. The online submission must be signed by the highest-ranking executive at the Covered Entity and the Covered Entity's Chief Information Security Officer ("CISO"). If a Covered Entity does not have a CISO, then the senior officer responsible for the cybersecurity program must sign the annual compliance. Documentation supporting this compliance must be maintained for five years.

Attorneys

Sabrina Janeiro

Cathy Mulrow-Peattie

Service Areas

Consumer Financial Services

Privacy, Security & Artificial Intelligence

Additional Technical Requirements for Covered Entities and Class A Companies That Must be in Place by May 1, 2025

Covered Entities and Class A Businesses must comply with additional technical cybersecurity control requirements under 23 NYCRR 500. **The following requirements apply to both Covered Entities and Class A businesses:**

- Conduct "automated scans of information systems, and a manual review of systems not covered by such scans" to discover, analyze, and report vulnerabilities at a frequency determined by their risk assessment and promptly after any material system changes.
- Implement enhanced requirements regarding limiting user access privileges, including privileged account access.
- Review access privileges and remove or disable accounts and access that are no longer necessary.
- Disable or securely configure all protocols that permit remote control of devices.
- Promptly terminate access following personnel departures.
- Implement a reasonable written password policy to the extent passwords are used.

The following additional requirements apply to Class A businesses as of May 1:

- Monitor privileged access activity.
- Implement a privileged access management solution.
- Implement an automated method of blocking commonly used passwords.
- Implement controls to protect against malicious code.
- Implement endpoint detection and response solution to monitor anomalous activity and centralized logging and security event alert solution.

Please remember to document all these controls.

MFA and Asset Inventory Procedures That Must be in Place by November 1, 2025

Covered Entities and Class A businesses should be working towards implementing the following requirements by November 1, 2025:

- Implement multi-factor authentication for all individuals accessing information systems.
- Implement written policies and procedures designed to produce and maintain a complete, accurate, and documented asset inventory of information systems. Policies and procedures must include a method for tracking specified key information for each asset, such as the owner and location, and the frequency required to update and validate its asset inventory.

For questions, please contact Hinshaw's Privacy, Security, & Artificial Intelligence team.