Part 500 Requirement Checklist for DFS-Regulated Entities with § 500.19(a) Limited Exemptions*

Annual Requirements

☐ **File Annual Cybersecurity Compliance Forms** *(by April 15 of each year)*

Covered Entities must review data and documentation to determine their compliance with Part 500 for the prior year and submit either:

(i) A written certification of compliance certifying that the entity materially complied with the requirements of Part 500 during the prior calendar year, or

(ii) A written acknowledgement of noncompliance acknowledging that the entity did not materially comply with all the requirements of Part 500 during the prior calendar year, identifying all sections of Part 500 the entity did not materially comply with, and providing a remediation timeline or confirmation that remediation has been completed. (§ 500.17(b))

☐ **Review and Approve Written Cybersecurity Policies** *(by April 29 of each year)*

Covered Entities must annually review and approve their written cybersecurity policies. (§ 500.3)

☐ **Review and Update Risk Assessment** *(by April 29 of each year)*

Covered Entities must review and update their cybersecurity risk assessments at least annually, and when there is a material change to cyber risk. For example, review and update your risk assessment if your business has a significant change, or you significantly change the hardware or software you use to run your business. (§ 500.9(a))

☐ **Cybersecurity Awareness Training** *(by November 1 of each year)*

Covered Entities must provide all staff at least annual cybersecurity awareness training that includes social engineering. (§ 500.14(a)(3))

☐ **Review and Manage User Access Privileges** *(by May 1 of each year beginning in 2025)*

Effective now, Covered Entities must limit and review access privileges for users (including third-party service providers) that have access to nonpublic information maintained on their information systems. Beginning May 1, 2025, Covered Entities must review the access privileges of all users who have access to their information systems at least annually and determine whether they still need access, limit the access to only what they need, and terminate access that is no longer necessary. (§ 500.7(a)(4))

Additional and Ongoing Requirements

☐ Perform third-party service provider assessments on the continued adequacy of their cybersecurity practices. (§ 500.11(a)(4))

☐ Report cybersecurity incidents and extortion payments and provide required information regarding them. (§ 500.17(a), 500.17(c))

☐ Securely dispose of nonpublic information (NPI) that is no longer needed. (§ 500.13(b)

☐ Implement multifactor authentication (MFA) for remote access to your entity's information systems, remote access to third-party applications from which NPI is accessible, and all privileged accounts by November 1, 2024. Covered Entities that have CISOs who have approved the use of compensating controls in place of MFA must have their CISOs annually review and reapprove them. (§ 500.12)

☐ Develop and maintain up-to-date asset inventory of information systems beginning November 1, 2025. (§ 500.13(a)(2))

*This checklist is designed to help DFS-regulated entities who qualify for the limited exemption under § 500.19(a) of 23 NYCRR Part 500 achieve compliance with applicable sections of Part 500 once such sections take effect.

Covered Entities qualify for the limited exemption under Section 500.19(a) if they have:

(i) Fewer than 20 employees and independent contractors of the Covered Entity and its affiliates;
(ii) Less than $7,500,000 in gross annual revenue in each of the last three fiscal years from all business operations of the Covered Entity and the business operations in New York State; or
(iii) Less than $15,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates.