Cybersecurity Program Template

A resource to help individual licensees and individually owned businesses develop a cybersecurity program as required by New York State's Cybersecurity Regulation 23 NYCRR Part 500.

Name:

Date Updated:

May 2024

Table of Contents

Overview

Disclaimer: This template is not a substitute for independently evaluating any business, legal, or other issues, and completing the template does not assure that any individual licensee is in compliance with the requirements of the Cybersecurity Regulation. Rather, the template asks questions that prompt individual licensees to think about and address the core concepts of a cybersecurity program to help implement a program that complies with the requirements of the Cybersecurity Regulation. See the questions below for additional information.

What is the Cybersecurity Program Template?

This template is provided by the New York State Department of Financial Services (DFS) as a tool to help individual licensees and individually owned businesses licensed by DFS (collectively, individual licensees) in developing a cybersecurity program as required by 23 NYCRR Part 500, the DFS Cybersecurity Regulation.

This document does not need to be submitted to DFS or any other state agencies for approval.

Throughout the template, you will see underlined phrases, which are defined in Appendix 1: Definitions of Key Terms. You will also see "Section" or "§" followed by the part of the Cybersecurity Regulation that requirement applies to, which you can refer to for more information.

Who should use this resource?

This template is intended for individual licensees who qualify for a section 500.19(a) limited exemption under the Cybersecurity Regulation, meaning:

- (1) The individual licensee and its affiliates combined have fewer than 20 employees and independent contractors;
- (2) The individual licensee must have less than $7,500,000 in gross annual revenue in each of the last three fiscal years from all business operations of the licensee and the business operations of its affiliates in New York State; or
- (3) The individual licensee must have less than $15,000,000 in year-end total assets, including assets of all affiliates.

What laws and regulations are addressed by this resource?

DFS is providing this template to assist individual licensees in complying only with the Cybersecurity Regulation. It does not consider any other law or regulation that may apply to an individual licensee's business. Individual licensees should carefully review applicable laws and regulations in all jurisdictions where they do business in structuring their cybersecurity programs, including applicable breach notification and privacy laws. If specific advice is required or desired, the services of an appropriate, competent professional should be sought.

This template was prepared based on the version of the DFS Cybersecurity Regulation in effect as of November 1, 2023. Please note that the requirements of the Cybersecurity Regulation may be amended in the future, in which case this template may no longer accurately reflect the requirements of the Cybersecurity Regulation. Be sure to periodically check DFS's Cybersecurity Resource Center, available at www.dfs.ny.gov/cyber, for any changes to the Cybersecurity Regulation or this template.

Where can I get additional support to ensure I am compliant with the Cybersecurity Regulation?

DFS's Cybersecurity Resource Center includes the regulation, training resources, FAQs, and more to help you understand and comply with the Cybersecurity Regulation. You can also receive important regulatory guidance, cybersecurity alerts, and other information related to cybersecurity in the financial services sector by going to the DFS Email Updates Signup Page available at https://on.ny.gov/subscribenydfs and subscribing to Cybersecurity Updates. These emails will come from the email address nydfs@public.govdelivery.com.

Instructions

1. If you are an individual licensee, first check to see if you need to comply with DFS's Cybersecurity Regulation.
    - You can check DFS's Cybersecurity Resource Center under the section "Producers, Individual Licensees and Small Businesses."
    - If you qualify for a limited exemption under section 500.19(a) (see "Who should use this resource?" on the prior page), this template is designed for you.
    - Note: If you are fully exempt from the Cybersecurity Regulation under sections 500.19(b), (e) or (g), you are NOT required to have a Cybersecurity Program and therefore do not need to fill this out. However, because cybersecurity risks affect everyone, you may want to consider the template as you decide how best to protect yourself, your clients, and consumers. If you are exempt, please be sure to notify DFS of your exemption status. You can find instructions for how to do so at https://on.ny.gov/Part500Exemptions.
2. Set aside a few hours to review and complete this template.
    - To complete the template, you will need information about your technology devices, including your laptop, desktop, server, printer, copier/fax, and smartphone and software services, including email hosting, billing provider, and website hosting.
3. After you complete the template, keep it in a safe place and use it to help guide your cybersecurity efforts.
    - DFS does not expect you to send or submit the completed template. Review and update the completed template annually and whenever your business or operations significantly change.

I. Cybersecurity Program Information

1. Who is involved in managing your information systems? For an individual, information systems likely will include your technology devices such as your laptop, desktop, server, printer, copier/fax, and smartphone and software services such as email hosting, billing provider, and website hosting. (Check all that apply.)

- [ ] Me
- [ ] Third-party consultant or company
- [ ] Other (describe below)

If someone other than you is involved, describe how you divide responsibilities to manage your information systems:

2. Who is responsible for maintaining the cybersecurity of your information systems? (Check all that apply.)

- [ ] Me
- [ ] Third-party consultant or company
- [ ] Other (describe below)

If someone other than you is responsible, please describe what they are responsible for and provide their contact information below:

II. Asset Inventory

If you do not already have an inventory of your information systems, first complete the asset inventory template provided in Appendix 2.

1. Generally, an asset inventory should be reviewed annually and when there is a significant change in how your business operates. How often is the asset inventory updated and checked for accuracy?

- [ ] At least annually and when there is a significant change.
- [ ] Less frequently than annually. (Explain why.)

2. Where do you keep this asset inventory, so it is available in case of a disaster or other disruptive event?

III. Cybersecurity Risk Assessment

Cybersecurity risk assessments identify the potential cybersecurity hazards that could negatively affect your ability to conduct business, and the potential costs of a cybersecurity incident. They also take into account your specific circumstances, including the types of services and/or products you offer, your operations, customers, counterparties, service providers, vendors, location, and the type and amount of data you maintain. Section 500.9(a) of the Cybersecurity Regulation requires you to conduct a periodic cybersecurity risk assessment that is reviewed and updated as reasonably necessary, but at a minimum annually, and whenever a change in the business or technology causes a material change to your cyber risk.

Complete the cybersecurity risk assessment schedule in Appendix 3 and answer the following questions:

1. Date of last cybersecurity risk assessment:
2. Planned date of next cybersecurity risk assessment:

IV. Third-Party Service Providers

Section 500.11(a) requires you to periodically assess the adequacy of the cybersecurity practices of third-party service providers to ensure the security of your information systems and the nonpublic information accessible to, or held by, your third-party service providers. After you answer the following question, complete the third-party service provider table in Appendix 4, and review and update the information periodically.

1. Do you use any third-party service providers who have access to your nonpublic information? Include (i) the parties you identified in Section I above and (ii) any other third parties who have access to your information systems and the nonpublic information on them.
   - Yes
   - No

V. Access Privileges and Management

1. How do you ensure that users accessing information systems with nonpublic information, such as third-party service providers, are who they claim to be?
   - Users are required to authenticate themselves (for example, through a username and password).
   - Other (describe below)

2. If you allow third-party users to access information systems that provide access to nonpublic information, do you limit their access only to what's needed to perform their work?

- [ ] Yes
- [ ] No
- [ ] Other (describe below)

Section 500.7(a)(1) requires you to limit user access privileges to information systems that provide access to nonpublic information to only those necessary to perform the user's job.

3. If you answered yes to the previous question, do you periodically review and update this type of access and remove or disable accounts and access that are no longer necessary?

- [ ] Yes
- [ ] No
- [ ] N/A

Section 500.7(a)(4) requires you to review all user access privileges and remove or disable accounts and access that are no longer necessary at least once a year.

4. Do you use any type of remote access (for example, VPN from home to office computers)?

- [ ] Yes
- [ ] No

5. If you answered yes to the previous question, do you have controls in place to secure the remote connection (for example, VPN, firewalls, multi-factor authentication)?

- [ ] Yes
- [ ] No
- [ ] N/A

Section 500.7(a)(5) requires you to disable or securely configure all protocols that permit remote control of devices.

6. Do you use multi-factor authentication for all remote access to information systems?

- [ ] Yes
- [ ] No

As of November 1, 2024, you must use multi-factor authentication when an authorized user wants to access your information systems remotely. See Section 500.12(a)(1).

7. If you have a Chief Information Security Officer (CISO), have they approved in writing any exceptions to your use of multi-factor authentication?

- [ ] Yes (document all such exceptions on Appendix 5)
- [ ] No
- [ ] N/A

Section 500.12(b) permits your CISO – if you have one – to approve in writing the use of reasonably equivalent or more secure compensating controls. Such controls must be reviewed and revised, if necessary, at least once a year.

8. Do you promptly terminate access when third-party service providers or other users who have access to your information systems leave or terminate their relationship with your business?

- [ ] Yes
- [ ] No
- [ ] N/A

Section 500.7(a)(6) requires you to promptly terminate access following departures.

9. On information systems you control, such as your mobile devices or laptops, what password requirements do you have in place?

- [ ] Minimum character length (specify minimum character limit):
- [ ] No sequential characters (such as "1234") or repeated characters (such as "aaaa")
- [ ] Certain number of failed password attempts result in an account lock (specify number of attempts):
- [ ] Context-specific words, such as the name of the service or the individual's username, are not allowed.
- [ ] Other (specify):

Section 500.7(b) requires that if you use passwords as a method of authentication, you must have a written password policy that meets industry standards. More information on passwords is available from the U.S. Cybersecurity and Infrastructure Security Agency at https://www.cisa.gov/secure-our-world/require-strong-passwords.

VI. Data Retention and Disposal

Section 500.13(b) requires you to have policies and procedures for the secure disposal on a periodic basis of any nonpublic information that is no longer necessary for business operations or for other legitimate business purposes, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

1. Describe how you dispose of nonpublic information when it is no longer necessary for business operations or for other legitimate business purposes:

2. Describe how long nonpublic information is retained, both generally and for any special categories where the general rule does not apply:

Section 500.13(b) requires you to have policies and procedures for secure disposal on a periodic basis of any nonpublic information that is no longer necessary for business operations or for other legitimate business purposes, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Examples of secure disposal methods include: shredding paper so nonpublic information cannot be read or reconstructed; destroying or erasing electronic files or media so that non public information cannot be read or reconstructed; and hiring qualified third-party service provider who can provide such secure disposal. More information is available from the U.S. Cybersecurity and Infrastructure Security Agency at https://www.cisa.gov/sites/default/files/publications/DisposeDevicesSafely.pdf.

VII. Cybersecurity Awareness Training

As of November 1, 2024, you must participate in cybersecurity awareness training that includes social engineering at least once a year and that training must be updated to reflect risks identified by the covered entity in its cybersecurity risk assessment. See Section 500.14(a)(3).

1. Date of your most recent cybersecurity awareness training:

2. How often do you take cybersecurity awareness training?

- [ ] Annually (annual frequency is minimum required)
- [ ] Quarterly
- [ ] Monthly
- [ ] Other (describe below)

3. Does your cybersecurity awareness training explain the risks of, and help inform how to detect and not be fooled by, social engineering?

- [ ] Yes
- [ ] No

4. Is your cybersecurity awareness training updated to reflect risks identified by your cybersecurity risk assessment?

- [ ] Yes
- [ ] No

VIII. Incident Response and Reports

Section 500.17(a)(1) requires you to notify DFS of a cybersecurity incident within 72 hours of determining that a cybersecurity incident impacting your business has occurred. All cybersecurity incidents must be reported through the DFS Portal, available at https://myportal.dfs.ny.gov. Detailed instructions on reporting a cybersecurity incident are available on the Cybersecurity Resource Center.

1. Do you maintain an up-to-date list of everyone who needs to be contacted if you experience a cybersecurity incident? This may include an IT help desk company, significant customers and business partners, and cybersecurity insurance company.

- [ ] Yes
- [ ] No

If yes, where do you keep this list, so it is accessible in the event your information systems are not operational (such as in printed form or on a separate device)?

IX. Additional Policies

Section 500.3 requires your cybersecurity program to be based on your cybersecurity risk assessment and address the following areas to the extent they are applicable to your operations: (a) information security; (b) data governance, classification and retention; (c) asset inventory, device management and end of life management; (d) access controls, including remote access and identity management; (e) business continuity and disaster recovery planning and resources;(f) systems operations and availability concerns; (g) systems and network security and monitoring;(h) security awareness and training; (i) systems and application security and development and quality assurance; (j) physical security and environmental controls; (k) customer data privacy; (l) vendor and third-party service provider management; (m) cybersecurity risk assessment; (n) incident response and notification; and (o) vulnerability management.

To the extent any of the above areas are applicable to your operations and are not already addressed in this completed template, identify any additional policies or procedures you may have.

Appendix 1: Definitions of Key Terms

- Affiliate: Defined broadly to include almost all related companies. (§ 500.1(a))
- Asset Inventory: A comprehensive list of all hardware, software, network devices, and other technology assets within an organization. (§ 500.3(c))
- Chief Information Security Officer or CISO: A qualified individual who is responsible for overseeing and implementing a covered entity's cybersecurity program and enforcing its cybersecurity policy. (§ 500.1(c))
- Cybersecurity Incident: An occurrence where someone obtains unauthorized access to your information or information system or the information or information systems of your affiliates or third-party service providers that: (1) impacts you and requires you to notify any government body, self-regulatory agency or any other supervisory body; (2) has a reasonable likelihood of materially harming any material part of your normal operation(s); or (3) results in the deployment of ransomware within a material part of your information systems. (§§ 500.1(f) and (g))
- Information System: A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems. (§ 500.1(i))
- Multi-Factor Authentication: An electronic authentication method in which a user is granted access to a website or application only after successfully presenting two more factors such as a code, secret question, and/or password.
- Nonpublic Information: (i) Business-related information that would impact your business if stolen or tampered with, (ii) personally identifiable information, such as social security numbers, drivers' license numbers, and account numbers, and (iii) most health care related information or data (other than age or gender). (§ 500.1(k))
- Risk Assessment: An assessment that identifies the potential cybersecurity hazards that could negatively affect your ability to conduct business, and the potential costs of a cybersecurity incident. They also take into account your specific circumstances, including the types of services and/or products you offer, your operations, customers, counterparties, service providers, vendors, location, and the type and amount of data you maintain. (§ 500.1(p))
- Third-Party Service Providers: An individual or entity, including partnerships, corporations, branches, agencies, or associations, that is not an affiliate of the covered entity or a governmental entity, provides services to the covered entity, and maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the covered entity. (§ 500.1(m) and (s))

Appendix 2: Asset Inventory of Information Systems

Your written cybersecurity program is generally required to address your asset inventory, pursuant to § 500.3(c). As of November 1, 2025, your asset inventory must include a method to track certain key information for each information system, including its owner, location, classification or sensitivity, support expiration date, and recovery time objectives. (§ 500.13(a))

The table below is provided as a template and the information for all columns must be included, unless not applicable to the information system listed. For classification or sensitivity, you may wish to categorize the information system based on the information contained on the system, and use a label such as public, internal, or confidential to describe such information.

Include all applicable information systems you use here, including any:

- Hardware, such as servers, workstations, firewalls, wireless routers, mobile phones, printers, and copiers
- Software, such as operating systems (Windows 11, macOS 14, etc.) and applications (Microsoft Office, Adobe Acrobat, etc.)
- Cloud providers, such as G Suite, Azure, and AWS

Add any additional categories with information that is helpful. Additional categories you may want to include as part of this inventory, to the extent applicable, may include serial number, version, purchase date, and warranty information.

Information System	Owner	Location	Classification or Sensitivity (Public, Internal, or Confidential)	Support Expiration Date	Recovery Time Objectives	Other

Appendix 3: Risk Assessment

When completed, this template will be the risk assessment for your business. In other words, the completed template should help you identify cybersecurity risks and the controls used to mitigate such risks. Use this risk assessment to confirm that you have implemented the appropriate cybersecurity controls. You must review and update this risk assessment at least annually and as necessary to address changes to information systems, nonpublic information (NPI), or business operations.

What Am I Trying to Protect?	Risk	Controls Used to Reduce Risk (check all that apply)	Notes
NPI including customer information, passwords, and other sensitive information.	• Hackers trying to steal data (phishing, ransomware, etc.) • Insecure disposal of NPI • Defective/corrupt IT Other (describe):	☐ **Cybersecurity awareness training:** Keep up to date with new threats or changes in compliance requirements. ☐ **Use security software:** Install reputable antivirus and antimalware software and keep it updated to protect against threats from email and web browsing. ☐ **Regularly update software:** Keep all business-related software and systems up to date. ☐ **Multi-factor authentication:** This added layer of security is proven to be effective at significantly reducing the risk of unauthorized access, and as of November 1, 2024, you must use multi-factor authentication when an authorized user wants to access your information systems remotely. (§ 500.12(a)(1)) ☐ **Back up data regularly:** Regular backups can help you recover quickly from data loss due to cyberattacks or hardware failures. ☐ **Secure network:** Use a firewall and secure your Wi-Fi network. Use a Virtual Private Network (VPN) when accessing nonpublic data over public networks. ☐ **Develop a response plan:** Have a plan in place for responding to a cybersecurity incident.	

What Am I Trying to Protect	Risk	Controls Used to Reduce Risk (check all that apply)	Notes
		☐ **Use secure shredding/disposal service:** Destroy paper documents containing sensitive information and removable media such as USB drives should be physically destroyed if they contain sensitive information. ☐ **Sign up for cyber updates** (such as DFS Cyber Updates) ☐ Other (describe): ☐ Other (describe):	
Continuity of operations	• Ransomware • Defective/corrupt IT • Third-party supplier not able to deliver/operate • Other (describe)	☐ Plan how to respond to cybersecurity events and incidents. ☐ Plan how to continue or restore key business operations (maintain backups/ off-site storage, etc.) ☐ Other (describe): ☐ Other (describe):	
Physical theft/disruption	• Theft of laptop or other devices • Other types of physical harm to Data or IT assets • Other (describe)	☐ Laptop docking stations/locks ☐ Locked door access ☐ Locked closet/cabinets ☐ Building security ☐ Security cameras ☐ Other (describe): ☐ Other (describe):	
Other – add any here that are not already identified			

Appendix 4: Third-Party Service Providers

You are required to have written policies and procedures designed to ensure the security of your information systems and nonpublic information that are accessible to, or held by, third-party service providers (TPSP), such as your email service provider or payment processor. These policies and procedures must address, to the extent applicable and among other things, minimum cybersecurity practices the TPSP must have in place to do business with you, diligence processes used to evaluate the adequacy of their cybersecurity practices, and the frequency required to reassess their cybersecurity practices (based on the risk they present). (§ 500.11(a))

The table below is provided as a template – use it as relevant and applicable. Examples of due diligence that, if relevant and applicable, can be performed to evaluated cybersecurity practices of a TPSP include:

- ☐ Confirm TPSP uses multi-factor authentication when accessing my organization's information.
- ☐ Confirm TPSP uses encryption policies and procedures to protect nonpublic information.
- ☐ Confirm TPSP contract includes requirements to notify me if there is a cybersecurity incident.
- ☐ Overall assessment that TPSP is appropriate to provide the service, considering the type of service provided and the TPSP's position in the market (such as size, reputation, cybersecurity program).
- ☐ Other (describe):

Third-Party Service Provider (Name and Contact)	Level of Risk Posed (Low, Medium, High)	Due Diligence Performed to Evaluate Their Cybersecurity Practices	Frequency of Assessment (Frequency Based on Level of Risk Posed)	Other
Email service provider:				
Payment processor:				

Appendix 5: Multi-Factor Authentication Exceptions

Section 500.12(b) permits your CISO – if you have one – to approve in writing the use of reasonably equivalent or more secure compensating controls. Such controls must be reviewed and revised, if necessary, at least once a year.

The table below is provided as a template. If you have a CISO, list any exceptions to your use of multi-factor authentication that your CISO approved in writing. Add any additional categories with information that is helpful.

Date Exception Granted	Information System and Account	Reason	Compensating Controls	Date of Last Review

Appendix 6: Cybersecurity Timeline Implementation for Small Businesses

Download and print this full resource from DFS's Cybersecurity Resource Center.

This timeline includes key dates for DFS-licensed individual producers, mortgage loan originators, and other businesses that qualify for exemptions under Sections 500.19 (a), (c), and (d) of the amended Cybersecurity Regulation.

Cybersecurity Implementation Timeline for Small Businesses

This timeline includes key dates for DFS-licensed individual producers, mortgage loan originators, and other businesses that qualify for exemptions under Sections 500.19 (a), (c), and (d) of the amended Cybersecurity Regulation.

**Indicates actions that are not required for Covered Entities that qualify for 500.19(c) and (d) exemptions. 500.19(c) exemptions apply to entities that do not maintain nonpublic information and 500.19(d) exemptions apply to captive insurers.*

This guide is provided for general planning purposes. Please consult the text of the Cybersecurity Regulation for specific requirements.

December 1, 2023
Section 500.17
Notifying DFS of cybersecurity events continues to be required. What's new: Ransomware deployment and any ransom payments made must be reported.

April 29, 2024
Section 500.9
• Risk assessments continue to be required. What's new: Risk assessments must be reviewed and updated at least annually, and whenever a change in the business or technology causes a material change to the business' cyber risk.

Section 500.3*
• After assessing your risks, update your policies to address these issues if needed:
- Data retention
- End of life management (phasing out unsupported technical products with vulnerabilities)
- Remote access controls
- Systems and network monitoring
- Security awareness and training
- Systems and application security
- Incident notification
- Vulnerability management

November 1, 2025
Section 500.12*
Comply with enhanced MFA requirements.

Section 500.13(a)
Implement new asset inventory requirements.

November 1, 2023
Section 500.19
More businesses qualify for exemptions (limited and full). Check to confirm eligibility for an exemption.

April 15, 2024
Section 500.17(b)
Annual compliance submissions continue to be due. What's new: Determine whether to file one of two new forms: Certification of Material Compliance or Acknowledgment of Noncompliance.

November 1, 2024
Section 500.12(a)*
Implement multifactor authentication (MFA) requirements outlined in Section 500.12(a) if you have not already done so.

Section 500.14(a)(3)*
Provide all personnel at your business at least annual cybersecurity awareness training.

May 1, 2025
Section 500.7*
• 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 you use passwords.

NOVEMBER 2023

Appendix 7: Part 500 Requirement Checklist for DFS-Regulated Entities with § 500.19(a) Limited Exemptions

Download and print this full resource, which highlights annual and ongoing requirements for individual licensees who qualify for a section 500.19(a) limited exemption, from DFS's Cybersecurity Resource Center.

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))

Visit the Department of Financial Services' Cybersecurity Resource Center for additional information on the above requirements and resources to aid with Part 500 compliance.
www.dfs.ny.gov/cyber
February 2024

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.

Visit the Department of Financial Services' Cybersecurity Resource Center for additional information on the above requirements and resources to aid with Part 500 compliance.
www.dfs.ny.gov/cyber
February 2024

Appendix 8: Cybersecurity Regulation Exemption Flowchart

Download and print this full resource from DFS's Cybersecurity Resource Center.