NYS DFS Part 500 - 23 NYCRR Part 500

Policies and Procedures

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

Table of Contents

27	NYS DFS Part 500 500.11(a) - Third Party Service Provider Security Policy - Policies and procedures
28	NYS DFS Part 500 500.11(b) - Third Party Service Provider Security Policy - Contractual protections
29	NYS DFS Part 500 500.11(c) - Third Party Service Provider Security Policy - Limited exception
30	NYS DFS Part 500 500.12(a) - Multi-Factor Authentication - Optional
31	NYS DFS Part 500 500.12(b) - Multi-Factor Authentication - Required
32	NYS DFS Part 500 500.13 - Limitations on Data Retention
33	NYS DFS Part 500 500.14 - Training and Monitoring - Actvity monitoring
34	NYS DFS Part 500 500.14 - Training and Monitoring - Training
35	NYS DFS Part 500 500.15(a) - Encryption of Nonpublic Information
36	NYS DFS Part 500 500.15(a)(1) - Encryption of Nonpublic Information - In-transit exception
37	NYS DFS Part 500 500.15(a)(2) - Encryption of Nonpublic Information - At-rest exemption
38	NYS DFS Part 500 500.15(b) - Encryption of Nonpublic Information - annual review
39	NYS DFS Part 500 500.16(a) - Incident Response Plan - Written plan
40	NYS DFS Part 500 500.16(b) - Incident Response Plan - Contents
41	NYS DFS Part 500 500.17(a) - Notices to Superintendent - 72-hour reporting
42	NYS DFS Part 500 500.17(b) - Notices to Superintendent - Annual report
43	NYS DFS Part 500 500.18 - Confidentiality
44	NYS DFS Part 500 500.19 - Exemptions

Purpose

The purpose is to ensure that all qualifying businesses that are supervised by the New York State Department of Financial Services meet all the requirements defined in 23 NYCRR Part 500.

Scope

This policy applies to the workforce members and vendors of organizations that come in contact with sensitive, confidential, and/or protected data.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

NYS DFS Part 500 500.01 - Definitions

NYS DFS Part 500 - 23 NYCRR Part 500	Other Requirements
500.01 Definitions	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

(a) Affiliate means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

(b) Authorized User means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

(c) Covered Entity means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

(d) Cybersecurity Event means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

(e) Information System means 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.

(f) Multi-Factor Authentication means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password; or

(2) Possession factors, such as a token or text message on a mobile phone; or

(3) Inherence factors, such as a biometric characteristic.

(g) Nonpublic Information shall mean all electronic information that is not Publicly Available Information and is:

(1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;

(2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;

(3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

(h) Penetration Testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems.

(i) Person means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

(j) Publicly Available Information means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

(1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(k) Risk Assessment means the risk assessment that each Covered Entity is required to conduct under section 500.09 of this Part.

(l) Risk-Based Authentication means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

(m) Senior Officer(s) means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part.

(n) Third Party Service Provider(s) means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

Guidance
Understand the definitions to ensure your compliance.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- NYDFS-1 - Definitions: (a) Affiliate means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise. (b) Authorized User means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity. (c) Covered Entity means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law. (d) Cybersecurity Event means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System. (e) Information System means 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. (f) Multi-Factor Authentication means authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; or (2) Possession factors, such as a token or text message on a mobile phone; or (3) Inherence factors, such as a biometric characteristic. (g) Nonpublic Information shall mean all electronic information that is not Publicly Available Information and is: (1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity; (2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual. (h) Penetration Testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems. (i) Person means any individual or any non-governmental entity, including but not limited to any non- governmental partnership, corporation, branch, agency or association. (j) Publicly Available Information means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law. (1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine: (i) That the information is of the type that is available to the general public; and (ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so. (k) Risk Assessment means the risk assessment that each Covered Entity is required to conduct under section 500.09 of this Part. (l) Risk-Based Authentication means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions. (m) Senior Officer(s) means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part. (n) Third Party Service Provider(s) means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or

otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

References

- Text of Regulation - https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
- NY Dept. of Financial Services Cybersecurity Resource Center - https://www.dfs.ny.gov/industry_guidance/cybersecurity
- FAQs: 23 NYCRR Part 500 - https://www.dfs.ny.gov/industry_guidance/cyber_faqs

NYS DFS Part 500 500.02(a) - Cybersecurity Program - Confidentiality, integrity and availability

NYS DFS Part 500 - 23 NYCRR Part 500	Other Requirements
500.02(a) Cybersecurity Program - Confidentiality, integrity and availability	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.

Guidance
This regulation is modeled after the NIST Cybersecurity Framework (CSF). By implementing the NIST CSF controls you will meet the New York Department of Financial Services requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- NYDFS-2 - Cybersecurity Program: Maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of your Information Systems.

References
- Text of Regulation - https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
- NY Dept. of Financial Services Cybersecurity Resource Center - https://www.dfs.ny.gov/industry_guidance/cybersecurity
- FAQs: 23 NYCRR Part 500 - https://www.dfs.ny.gov/industry_guidance/cyber_faqs

NYS DFS Part 500 500.02(b)(1) - Cybersecurity Program - Risks

NYS DFS Part 500 - 23 NYCRR Part 500	Other Requirements
500.02(b)(1) Cybersecurity Program - Risks	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems.

Guidance
This regulation is modeled after the NIST Cybersecurity Framework (CSF). By implementing the NIST CSF Identification and risk assessment controls you will meet the New York Department of Financial Services requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC5.1 - Risk Assessment/Risk Analysis: Periodically conduct an accurate and thorough assessment of the risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of data.
- CC14.1 - Business Continuity & Disaster Recovery Plans: Write effective Business Continuity and Disaster Recovery plans that meet all regulatory requirements and are in place and managed.
- CC18.3 - Response Procedures: Develop and implement responses to declared incidents according to pre-defined procedures.

References
- Text of Regulation - https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
- NY Dept. of Financial Services Cybersecurity Resource Center - https://www.dfs.ny.gov/industry_guidance/cybersecurity
- FAQs: 23 NYCRR Part 500 - https://www.dfs.ny.gov/industry_guidance/cyber_faqs

NYS DFS Part 500 500.02(b)(2) - Cybersecurity Program - Protection

NYS DFS Part 500 - 23 NYCRR Part 500	Other Requirements
500.02(b)(2) Cybersecurity Program - Protection	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

Guidance
This regulation is modeled after the NIST Cybersecurity Framework (CSF). By implementing the NIST CSF Protect function controls you will meet the New York Department of Financial Services requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC3.2 - Governance & Risk Management Processes: Ensure governance and risk management processes address cybersecurity risks.
- CC4.1 - Written Cybersecurity Policies: Write policies addressing all cybersecurity requirements.
- CC4.3 - Written Procedures: Create written documentation for each procedure.

References
- Text of Regulation - https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
- NY Dept. of Financial Services Cybersecurity Resource Center - https://www.dfs.ny.gov/industry_guidance/cybersecurity
- FAQs: 23 NYCRR Part 500 - https://www.dfs.ny.gov/industry_guidance/cyber_faqs

NYS DFS Part 500 500.02(b)(3) - Cybersecurity Program - Detection

NYS DFS Part 500 - 23 NYCRR Part 500	Other Requirements
500.02(b)(3) Cybersecurity Program - Detection	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(3) detect Cybersecurity Events

Guidance
This regulation is modeled after the NIST Cybersecurity Framework (CSF). By implementing the NIST CSF Detect function controls you will meet the New York Department of Financial Services requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC18.1 - Detect Events: Detect and report events.

References
- Text of Regulation - https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
- NY Dept. of Financial Services Cybersecurity Resource Center - https://www.dfs.ny.gov/industry_guidance/cybersecurity
- FAQs: 23 NYCRR Part 500 - https://www.dfs.ny.gov/industry_guidance/cyber_faqs

NYS DFS Part 500 500.02(b)(1) - Cybersecurity Program - Response

NYS DFS Part 500 - 23 NYCRR Part 500	Other Requirements
500.02(b)(1) Cybersecurity Program - Response	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

Guidance
This regulation is modeled after the NIST Cybersecurity Framework (CSF). By implementing the NIST CSF Response function controls you will meet the New York Department of Financial Services requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC5.1 - Risk Assessment/Risk Analysis: Periodically conduct an accurate and thorough assessment of the risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of data.
- CC14.1 - Business Continuity & Disaster Recovery Plans: Write effective Business Continuity and Disaster Recovery plans that meet all regulatory requirements and are in place and managed.
- CC18.3 - Response Procedures: Develop and implement responses to declared incidents according to pre-defined procedures.

References
- Text of Regulation - https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
- NY Dept. of Financial Services Cybersecurity Resource Center - https://www.dfs.ny.gov/industry_guidance/cybersecurity
- FAQs: 23 NYCRR Part 500 - https://www.dfs.ny.gov/industry_guidance/cyber_faqs

NYS DFS Part 500 500.02(b)(1) - Cybersecurity Program - Recover

NYS DFS Part 500 - 23 NYCRR Part 500	Other Requirements
500.02(b)(1) Cybersecurity Program - Recover	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(5) recover from Cybersecurity Events and restore normal operations and services

Guidance
This regulation is modeled after the NIST Cybersecurity Framework (CSF). By implementing the NIST CSF Recover function controls you will meet the New York Department of Financial Services requirements.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC5.1 - Risk Assessment/Risk Analysis: Periodically conduct an accurate and thorough assessment of the risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of data.
- CC14.1 - Business Continuity & Disaster Recovery Plans: Write effective Business Continuity and Disaster Recovery plans that meet all regulatory requirements and are in place and managed.
- CC18.3 - Response Procedures: Develop and implement responses to declared incidents according to pre-defined procedures.

References
- Text of Regulation - https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
- NY Dept. of Financial Services Cybersecurity Resource Center - https://www.dfs.ny.gov/industry_guidance/cybersecurity
- FAQs: 23 NYCRR Part 500 - https://www.dfs.ny.gov/industry_guidance/cyber_faqs

NYS DFS Part 500 500.02(c) - Cybersecurity Program - Affiliates

NYS DFS Part 500 - 23 NYCRR Part 500	Other Requirements
500.02(c) Cybersecurity Program - Affiliates	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

(c) A Covered Entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity.

Guidance
Affiliate means any Person that controls, is controlled by or is under common control with another Person. Control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

Affiliates include subsidiaries, agents (including insurance agents), local financial advisors for national firms, etc.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- NYDFS-3 - Cybersecurity Program - Affiliates: Adopt the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy your requirements.

References
- Text of Regulation - https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
- NY Dept. of Financial Services Cybersecurity Resource Center - https://www.dfs.ny.gov/industry_guidance/cybersecurity
- FAQs: 23 NYCRR Part 500 - https://www.dfs.ny.gov/industry_guidance/cyber_faqs

NYS DFS Part 500 500.02(d) - Cybersecurity Program - Documentation

NYS DFS Part 500 - 23 NYCRR Part 500	Other Requirements
500.02(d) Cybersecurity Program - Documentation	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

(d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

Guidance
In a regulatory environment, evidence of compliance requires written documentation, that must be provided to regulators as requested.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- NYDFS-4 - Cybersecurity Program - Documentation: Create documentation relative to your cybersecurity program and provide to the NYS Department of Financial Services superintendent upon request.

References
- Text of Regulation - https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
- NY Dept. of Financial Services Cybersecurity Resource Center - https://www.dfs.ny.gov/industry_guidance/cybersecurity
- FAQs: 23 NYCRR Part 500 - https://www.dfs.ny.gov/industry_guidance/cyber_faqs

NYS DFS Part 500 500.03 - Cybersecurity Policy

NYS DFS Part 500 - 23 NYCRR Part 500	Other Requirements
500.03 Cybersecurity Policy	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:

(a) information security;

(b) data governance and classification;

(c) asset inventory and device management;

(d) access controls and identity management;

(e) business continuity and disaster recovery planning and resources;

(f) systems operations and availability concerns;

(g) systems and network security;

(h) systems and network monitoring;

(i) systems and application development and quality assurance;

(j) physical security and environmental controls;

(k) customer data privacy;

(l) vendor and Third Party Service Provider management;

(m) risk assessment; and

(n) incident response.

Guidance

A comprehensive written security policy covering the requirements in the NIST CSF and the more specific Part 500 requirements must be created, implemented, and maintained.

This policy (policies) must be formally approved by the organization's Senior Officer (executive or owner), Board of Directors (or a board committee) or similar governing body.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- NYDFS-5 - Cybersecurity Policy: Create, implement, and maintain a comprehensive written security policy covering the requirements in the NIST CSF and the more specific NYS Department of Financial Services Part 500 requirements. This policy (policies) must be formally approved by your Senior Officer (executive or owner), Board of Directors (or a board committee) or similar governing body.

References

- Text of Regulation - https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)
- NY Dept. of Financial Services Cybersecurity Resource Center - https://www.dfs.ny.gov/industry_guidance/cybersecurity
- FAQs: 23 NYCRR Part 500 - https://www.dfs.ny.gov/industry_guidance/cyber_faqs

Truncated Sample Report