23 NYCRR 500 Technical Overview

A2 CYBERSECURITY, LLC

146 South Liberty Drive, Stony Point, NY 10980

+1(888) 600-6389

Info@A2cybersecurity.com

Table of Contents

Sec. 500.00 – Introduction

- Introduction of 23 NYCRR 500 from the New York State Department of Financial Services

Sec 500.01 – Definitions

- Definitions on specific terms used in the document.

Sec 500.02 – Cybersecurity Program

The Requirements:
(a) Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.
(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(I) Identify and assess cybersecurity risks regarding non-public information systems.

(II) Implement written policies and procedures to protect the I.T. system and access to non-public information systems.

(III) Analyze and monitor network security events and network traffic.

(IV) Identify and eliminate malicious network activity.

(V) Recover and restore normal network operations and services.

(VI) Fulfill applicable regulatory reporting procedures.

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

This is Covered:

A2 Cybersecurity Managed Security Service Platform provides cybersecurity programs implemented by certified network security analysts to effectively fulfill the needs of the NYCRR 500 cybersecurity requirements. The cybersecurity program will make use of automated network monitoring and alerting, on-call network security personnel, alongside the deployment of network intrusion detection systems, vulnerability detection systems, file tripwire systems, and multi-factor authentication. Documentation is strictly followed, and A2 Cybersecurity (Third-Party CISO) conducts monthly IT strategy meetings with covered entity to ensure clear communication and direction for the covered entity's information security cybersecurity program.

Sec 500.03 – Cybersecurity Policy

Requirements:
Maintain written cybersecurity policies and procedures establishing protection and maintenance of the covered entity's I.T. Infrastructure and retention of Nonpublic information.

The written cybersecurity policies will address:
(1) Information Security
(2) Data classification
(3) Network asset (any computer on the network) identification and management
(4) Access controls and identity management
(5) Business continuity and disaster recovery planning and resources
(6) Systems operations and availability concerns
(7) Systems and network security
(8) Systems and network monitoring
(9) Systems and application development and quality assurance
(10) Physical security and environmental controls
(11) Customer data privacy
(12) Vendor and third party service provider management
(13) Risk assessment
(14) Incident response

This is Covered:

When implementing A2 Cybersecurity MSSP services, A2 will first conduct an initial network risk assessment audit to form the framework for a stable network security program. A2 Cybersecurity will develop a set of written cybersecurity policies and procedures for the Covered Entity, and review these procedures and their effectiveness annually.

A2 Cybersecurity managed security service platform provides coverage for points: [1, 2, 4, 5, 6, 9, 12, 13, 14], implementation of a network IDS covers points: [3, 7, 8,], and A2 Cybersecurity network support services are able to fulfill the remaining points: [10, 11 .] All requirements will be defined in more detail within contractual agreements between the the Covered Entity and A2 Cybersecurity.

Sec 500.04 – Chief Information Security Officer

Requirements:

(a) Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity’s cybersecurity program and enforcing its cybersecurity policy. A third party service provider may be contracted as the I.T. C.I.S.O.
(b) The CISO of each covered entity shall report in writing at least annually to the covered

entity's board of director, or equivalent governing body. The CISO shall report on the covered entity's cybersecurity program and the material cybersecurity risks. The CISO shall consider to the extent applicable:

(1) Confidentiality of nonpublic information, and the integrity and security of the covered entity's information systems.
(2) Covered Entity' cybersecurity policies and procedures
(3) Material cyber risks to the covered entity
(4) Effectiveness of the covered entity's cybersecurity program.
(5) History of cybersecurity events and network security events involving the covered entity's protected I.T. systems.

This is Covered:

A2 Cybersecurity (Third-Party CISO) information security personnel meet regulations and qualifications for providing third-party CISO services in the state of New York. Requirements for [500.04 A, B] are both covered through A2 Cybersecurity's managed security service platform. The contractual obligations between A2 Cybersecurity third-party service provider and the Covered Entity will be established after the initial Risk Assessment has been performed.

Sec 500.05 – Penetration Testing and Vulnerability Assessments

Requirements:
This regulations mandates that vulnerability assessments have to be performed on the Covered Entity's network Information Systems, internal and external. These periodic vulnerability assessments are reported and reviewed alongside the Covered Entity's cybersecurity policy and annual cybersecurity report.

This is Covered:

A2 Cybersecurity routinely performs extensive network vulnerability assessments and generates monthly vulnerability reports using the updated ET-Pro OpenVAS threat feeds and penetration assessment tools. A2 Cybersecurity provides monthly vulnerability reports effectively illustrating and mitigating any detected vulnerabilities within the overall Information Systems and I.T. Infrastructure of the covered entity.

Sec 500.06 – Audit Trail

Requirements::
Covered entity's privileged nonpublic information and information systems must provide an audit of all system access and historically reconstruct material financial transactions, going back no less than *5 years*.
(1) Reconstruct material financial transactions and provide data redundancy.
(2) Include Audit trails for cybersecurity events that have a reasonable likelihood of harming any part of normal operations or cause material harm to the covered entity's normal operations.

This is Covered:

A2 Cybersecurity MSSP service provides risk assessment against the current network environment including privileged data retrieval and handling. The extent to which material financial records must be handled and stored will be determined alongside on the results of the annual risk assessment report.

Sec 500.07 – Access Privileges

Requirements:
Limit user access privileges to privileged information systems, and provide access to nonpublic information, these user access restrictions must be periodically reviewed by the CISO (or a qualified designee of the covered entity.

This is Covered:

A2 Cybersecurity MSSP service limits user access to privileged information and information systems, and provides necessary multifactor authentication on information systems where applicable.
See section 500.12 Mf-A

Sec 500.08 – Application Security

Requirements:
(a) Each Covered Entity’s cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity’s technology environment.
(b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designatee) of the Covered Entity.

This is Covered:

A2 Cybersecurity MSSP covers written policy and procedural guidelines detailing secure administration and development of any internal used applications by the Covered Entity, these guidelines are reviewed annually by the CISO and included in the cybersecurity report.

Sec 500.09 – Risk Assessment

Requirements:
Each Covered Entity has to perform a periodic Risk Assessment of the Covered Entity’s Information Systems. The Risk Assessment will be carried out following a written set of policies and procedures, designed to assess and review:

(1) Overall cybersecurity risk evaluation and threat management policies.

(2) Risk assessment tracking: access control, data integrity, confidentiality, and overall security of covered entity's privileged information systems.
(3) Procedures for assessing cybersecurity event Risk Value, and set of policies for properly handling cybersecurity risks based on their risk value and setting within the environment.

This is Covered:

A2 Cybersecurity deploys a unified security management tool, OSSIM, to effectively meet risk assessment requirements and eliminate network threats.
A2 Cybersecurity MSSP service provides risk assessment adapted to the Covered Entity's network environment and information systems. Security event Risk Value is determined from environmental context and OSSIM's correlation engine.
By analyzing all network activity, the OSSIM security appliance is able to connect related security events together and recognize patterns within network activity. In the event of a malicious network incident, automatic alerts are then sent to cybersecurity and intelligence personnel within the covered entity's organization.

Section 500.10 Cybersecurity Personnel and Intelligence.

Requirements:
Network cybersecurity personnel and intelligence personnel have to meet requirements in section 500.04(a) and also meet requirements set forth in 500.10. The requirements from this section state mandate the use of qualified cybersecurity analysts in order to genuinely satisfy the regulations set forth inside of the 23 NYC 500 cybersecurity bill.

This is Covered:

Our network security analysts all hold CISSP security certifications alongside years of experience working full time within the information security field. A2 Cybersecurity personnel meet requirements listed in detail in section 500.10 (a).

Section 500.11 Third Party Service Provider Security Policy.

This sections details third-party security service provider and covered entity relationship. These requirements will be addressed inside the initial contracts between parties.

Section 500.12 Multi-Factor Authentication.

Requirements::
Covered Entity must make use of multi-factor authentication methods to protect access to nonpublic information or information systems. In particular, any external access to internal privileged information systems must be secured using multi-factor authentication systems.

This is Covered:

A2 Cybersecurity is an official partner with Duo-Security and makes use of Duo-Security makes use for 2 factor user authentication and mfa (multi-factor authentication.)

Section 500.13 Limitations on Data Retention.

Requirements:
Written policies and procedures for secure disposal of any nonpublic information no longer necessary for business operation or for any legal purpose.

This is Covered:

A2 MSSP provides periodic secure destruction of nonpublic information that is no longer needed, as identified in section 500.01-02.

Section 500.14 Training and Monitoring.

Requirements:
(a) The cybersecurity program must be able to detect unauthorized access, and monitor and log authorized user access to nonpublic information systems.
(b) Provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

This is Covered:

A2 MSSP handles nonpublic information (as defined in section 500.02-03) authorization and access control, through the use of multi-factor authentication and cybersecurity awareness personnel training programs. Our MSSP service is able to detect unauthorized access to privileged information systems through the use of system log monitoring and network IDS alerts.

Section 500.15 Encryption of Nonpublic Information.

Requirements:
Establish policies and procedures outlining and guiding the use of cryptographic communication systems and software in order to maintain security and protect nonpublic information held or transmitted by the Covered Entity.

This is Covered:

Based on risk assessment results, strong cryptographic algorithms will be implemented when and where the Covered Entity is transmitting and storing nonpublic information. The CISO will perform semi-annual risk assessment on secure communication methods and data storage methods.

Section 500.16 Incident Response Plan.

Requirements:
Each covered entity must establish a written incident response plan, designed to respond to and recover from any cybersecurity event materially impacting the Covered Entity's information systems or general business operations.

This is Covered:

A2 MSSP mandates written response procedures to respond to and eliminate cybersecurity threats when they arise. The incident response plan will provide instructions for threat management based on event severity and impact. The written incident response plan will address all points detailed in section 500 .16 of the NYCRR 500 bill.

Section 500.17 Notices to Superintendent.

Requirements:
Notice of cybersecurity events determined to be malicious in activity must be sent to the NYDFS superintendent within 72 hours of detection.

This is Covered:

A2 Cybersecurity handles all real-time network traffic inspection. Automatic alert generation is employed through the use of OSSIM threat management system and real-time deep packet inspection. All suspicious or malicious network activity will be investigated and reported upon investigation.
A2 Cybersecurity interfaces with the threat intelligence community for updated IP reputation block lists and emerging network threats from around the globe.

Section 500.18 Confidentiality.

Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

Section 500.19 Exemptions.

Exhaustive list of exemptions to this bill.

Section 500.20 Enforcement.
This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent’s authority under any applicable laws.

Section 500.21 Effective Date.

Effective March 1 2017, annual certification of compliance with NY Department of Financial services cybersecurity regulations commencing under section 500.17(b) of this Part beginning February 15, 2018.

Section 500.22 Transitional Periods.

Important List of Scheduled Security Implementation Deadlines

http://dfs.ny.gov/about/cybersecurity.htm

Section 500.23 Severability.

If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.