LIGHTHOUSE
COMPUTER SERVICES

Client Advisory:

New York State Department of Financial Services Cyber Security Requirements – Title 23 NYCRR Part 500

ALERT: As of March 1, 2017, the State of New York began to roll out new cyber security regulations impacting all institutions doing business with the state, regardless of their physical location.

These regulations are set forth in Title 23 NYCRR Parts 500.2 through 500.16, and are summarized in this publication.

Lighthouse urges you to consult with your compliance officer or counsel with compliance oversight to determine if and how these regulations apply to your firm.

NY State Cybersecurity Guidelines	Description	Risk Management Controls	Lighthouse Security Services
Section 500.02 Cybersecurity Program.	Cybersecurity Program. Each Covered Entity shall establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of the Covered Entity's Information Systems	Security Program	Security Strategy and Planning, 10 EPs Security Architecture and Product Design
	Each Covered Entity shall implement and maintain a written cybersecurity policy setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems.	Security Program	Security Policy, Audit and Compliance Mgmt
	The cybersecurity policy shall be reviewed by the Covered Entity's board of directors or equivalent governing body, and approved by a Senior Officer of the Covered Entity. If no such board of directors or equivalent governing body exists, the cybersecurity policy shall be reviewed and approved by a Senior Officer of the Covered Entity. Such review and approval shall occur as frequently as necessary to address the cybersecurity risks applicable to the Covered Entity, but no less frequently than annually.		
Section 500.04 Chief Information Security Officer.	Chief Information Security Officer. Each Covered Entity shall designate a qualified individual to serve as the Covered Entity's Chief Information Security Officer ("CISO") responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy.	Security Program	Security Strategy and Planning
	The CISO of each Covered Entity shall develop a report, at least bi-annually, as described herein. Such report shall be timely presented to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. Such report shall be made available to the superintendent upon request.		
Section 500.05 Penetration Testing and Vulnerability Assessments.	(a) The cybersecurity program for each Covered Entity shall, at a minimum, include: (1) penetration testing of the Covered Entity's Information Systems at least annually; and (2) vulnerability assessment of the Covered Entity's Information Systems at least quarterly.	Vulnerability Management	Active Threat Assessment Penetration Testing
Section 500.06 Audit Trail.	The cybersecurity program for each Covered Entity shall, at a minimum, include implementing and maintaining audit trail systems that: (1) track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting necessary to enable the Covered Entity to detect and respond to a Cybersecurity Event; (2) track and maintain data logging of all privileged Authorized User access to critical systems; (3) protect the integrity of data stored and maintained as part of any audit trail from alteration or tampering; (4) protect the integrity of hardware from alteration or tampering, including by limiting electronic and physical access permissions to hardware and maintaining logs of physical access to hardware that allows for event reconstruction; (5) log system events including, at a minimum, access and alterations made to the audit trail systems by the systems or by an Authorized User, and all system administrator functions performed on the systems; and (6) maintain records produced as part of the audit trail for not fewer than six years.	Security Intelligence	Security Operations Consulting SIEM Design and Deploy
Section 500.07 Access Privileges.	As part of its cybersecurity program, each Covered Entity shall limit access privileges to Information Systems that provide access to Nonpublic Information solely to those individuals who require such access to such systems in order to perform their responsibilities and shall periodically review such access privileges.	Privileged User Management Identity & Access Governance	Identity Governance and Administration Strategy, Design and Deploy
Section 500.08 Application Security.	(a) Each Covered Entity's cybersecurity program shall, at a minimum, 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, as well as procedures for assessing and testing the security of all externally developed applications utilized by the Covered Entity. (b) All such procedures, guidelines and standards shall be reviewed, assessed and updated by the CISO of the Covered Entity at least annually.	Dynamic Vulnerability Analysis Static Source Code Analysis	Hosted Application Security Management
Section 500.09 Risk Assessment.	(a) At least annually, each Covered Entity shall conduct a risk assessment of the Covered Entity's Information Systems. Such risk assessment shall be carried out in accordance with written policies and procedures and shall be documented in writing. (b) As part of such policies and procedures, each Covered Entity shall include, at a minimum: (1) criteria for the evaluation and categorization of identified risks; (2) criteria for the assessment of the confidentiality, integrity and availability of the Covered Entity's Information Systems, including the adequacy of existing controls in the context of identified risks; and 6 (3) requirements for documentation describing how identified risks will be mitigated or accepted based on the risk assessment, justifying such decisions in light of the risk assessment findings, and assigning accountability for the identified risks.	Risk Management	Security Framework and Risk Assessment

Section 500.10 Cybersecurity Personnel and Intelligence.	(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in 500.04(a), each Covered Entity shall: (1) employ cybersecurity personnel sufficient to manage the Covered Entity's cybersecurity risks and to perform the core cybersecurity functions specified in section 500.02(b)(1)-(5) of this Part; (2) provide for and require all cybersecurity personnel to attend regular cybersecurity update and training sessions; and (3) require key cybersecurity personnel to take steps to stay abreast of changing cybersecurity threats and countermeasures. (b) A Covered Entity may choose to utilize a qualified third party to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.	Security Program	Staff Augmentation Services Managed SIEM Managed and Hosted Services Incident Response Planning X-Force IRIS
Section 500.11 Third Party Information Security Policy.	Third Party Information Security Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, third parties doing business with the Covered Entity.	Risk Management	Security Framework and Risk Assessment
Section 500.12 Multi-Factor Authentication.	(a) Multi-Factor Authentication. Each Covered Entity shall: (1) require Multi-Factor Authentication for any individual accessing the Covered Entity's internal systems or data from an external network; (2) require Multi-Factor Authentication for privileged access to database servers that allow access to Nonpublic Information; (3) require Risk-Based Authentication in order to access web applications that capture, display or interface with Nonpublic Information; and (4) support Multi-Factor Authentication for any individual accessing web applications that capture, display or interface with Nonpublic Information.	Access Management	Mult-Factor Authentication Design and Deploy
Section 500.13 Limitations on Data Retention.	As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the timely destruction of any Nonpublic Information identified in 500.01(g)(2)-(4) that is no longer necessary for the provision of the products or services for which such information was provided to the Covered Entity, except where such information is otherwise required to be retained by law or regulation.	Data Protection	Critical Data Protection Program Resiliency Services
Section 500.14 Training and Monitoring.	(a) As part of its cybersecurity program, each Covered Entity shall: (1) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and 8 (2) provide for and require all personnel to attend regular cybersecurity awareness training sessions that are updated to reflect risks identified by the Covered Entity in its annual assessment of risks.	Access Control	Security Strategy and Planning Critical Data Protection Program
Section 500.15 Encryption of Nonpublic Information.	(a) As part of its cybersecurity program, each Covered Entity shall encrypt all Nonpublic Information held or transmitted by the Covered Entity both in transit and at rest. (b) To the extent encryption of Nonpublic Information in transit is currently infeasible, Covered Entities may instead secure such Nonpublic Information using appropriate alternative compensating controls reviewed and approved by the Covered Entity's CISO. Such compensating controls shall not be used in lieu of meeting the requirements of subsection 500.15(a) after one year from the date this regulation becomes effective. (c) To the extent encryption of Nonpublic Information at rest is currently infeasible, Covered Entities may instead secure such Nonpublic Information using appropriate alternative compensating controls reviewed and approved by the Covered Entity's CISO. Such compensating controls shall not be used in lieu of meeting the requirements of subsection 500.15(a) after five years from the date this regulation becomes effective.	Data Protection	DLP and Encryption Services
Section 500.16 Incident Response Plan.	As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business. (b) Such incident response plan shall, at a minimum, address the following areas: (1) the internal processes for responding to a Cybersecurity Event; (2) the goals of the incident response plan; (3) the definition of clear roles, responsibilities and levels of decision-making authority; (4) external and internal communications and information sharing; (5) remediation of any identified weaknesses in Information Systems and associated controls; (6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and (7) the evaluation and revision of the incident response plan following a Cybersecurity Event	Incident Response	IBM IRIS, Incident Response Planning Services
Section 500.17 Notices to Superintendent.	Each Covered Entity shall notify the superintendent of any Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information. The Covered Entity must notify the superintendent as promptly as possible but in no event later than 72 hours after becoming aware of such a Cybersecurity Event.	Incident Response	IBM IRIS

How the Lighthouse Security Practice can help

Lighthouse is an IBM Security Partner of long standing. We have the experience and expertise to help you ensure compliance by employing solutions that are robust and field proven.

For more information, please contact:
Scott C McNeil
Director of Security Sales
Lighthouse Computer Services
smcneil@lighthousecs.com

Since 1995, Lighthouse has provided expert counsel, implementation, and service for our clients' complex IT requirements.

Analytics
Cloud
DevOps
Infrastructure
Security
Business Productivity
Software Asset Management
Independent Discovery & Analytics (IDA)

LIGHTHOUSE
COMPUTER SERVICES

Lighthouse Computer Services, Inc. - www.lighthousecs.com
6 Blackstone Valley Place, Suite 205, Lincoln RI 02865 USA
100 Park Avenue, 16th Floor, New York NY 10017 USA