COMPLIANCE ADVISOR

New York Cybersecurity Regulation Compliance Guide

REVISED/REISSUED MAY 2022

A publication by:

THE EXCESS LINE ASSOCIATION OF NEW YORK

120 Wall Street | 24th Floor | New York, NY | 10005
(646) 292-5500 | elany@elany.org | www.elany.org

The New York Department of Financial Services (DFS) Cybersecurity Requirements for Financial Services Companies regulation (**23 CRR-NY 500**) became effective on March 1, 2017. THE REGULATION APPLIES TO ALL NEW YORK-LICENSED EXCESS LINE BROKERS — ENTITIES AND INDIVIDUALS, RESIDENT AND NONRESIDENT, REGARDLESS OF LINES OF INSURANCE BROKERED.

The following are the highlights for New York-licensed excess line brokers. A hyperlink to the regulation appears above for more in-depth detail regarding requirements. Each requirement is accompanied by the regulation section number being discussed. In addition, requirements that apply to exempt licensees are noted.

EXEMPTIONS (See §500.19 of the regulation)

Under **§500.19**, entity and individual licensees may avail themselves of **limited and full exemptions** from the regulation's requirements. Exemptions must be filed with the DFS via its **web portal**; unfiled exemptions are not valid. Filing instructions can be found **here**.[1] Upon filing, the DFS will not affirmatively grant an exemption; licensees are expected to properly determine eligibility for an exemption. Note that all but one exemption still require compliance with specified sections of the regulation. Licensees that do not qualify for an exemption must comply with all of the regulation's requirements. The following are the exemptions that may apply to excess line brokers, listed by regulation subsection:

§500.19(a) applies to New York-licensed excess line brokerages that are below specified thresholds in either number of employees located or responsible for business in New York, gross annual revenue from New York operations in each of the last three fiscal years, or total assets. Any licensee that qualifies for a §500.19(a) exemption need only comply with specified requirements, but these include substantial items such as implementing a cybersecurity program and policy, and performing periodic risk assessments.

- 500.19(a)(1) – A broker is entitled to this limited exemption when it has fewer than 10 employees, including independent contractors, who are "located in New York" or "responsible for business of the Covered Entity." The Covered Entity is the licensee. To determine the number, a licensee should add together:
  - all of its employees, regardless of location;
  - each **Affiliate** entity's employees who are located in New York; and
  - each Affiliate's employees who are responsible for any aspect of the licensee's business, regardless of the location of such employees. If an Affiliate's employee provides any service to, or performs any task for the licensee, that employee must be counted regardless of location. This includes, but is not limited to, any shared services provided by an Affiliate that are used by the licensee.
- 500.19(a)(2) – A broker is entitled to this limited exemption when it has had less than $5,000,000 in gross annual revenue in each of the last three (3) fiscal years from New York business operations. This includes the gross annual revenue from New York business operations of all Affiliates.
- 500.19(a)(3) – A broker is entitled to this limited exemption when it, plus all Affiliates regardless of location, have less than $10,000,000 in year-end total assets.

500.19(b) – A broker is entitled to this exemption when they are an employee, agent, representative or designee of another licensed entity and that entity's cybersecurity program is compliant with the regulation. This is a full exemption but it must be filed with the DFS.

[1] The DFS may permit a firm to make a coordinated filing of Notices of Exemptions on behalf of its New York-licensed employees or captive agents. This option is only available for filings of 50 or more employees or captive agents, and only if all employees or captive agents qualify for the same exemptions. A qualifying firm should contact the DFS at **CyberRegComments@dfs.ny.gov** from the email to which its cybersecurity portal account is associated. This **request** should be attached to the email.

500.19(c) – A broker is entitled to this limited exemption if it does not utilize an Information System[2] and does not, and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information[3]. Note that individuals who are currently licensed but not actively utilizing such license may fall into this category provided they are not maintaining Nonpublic Information concerning former or potential consumers or otherwise maintaining an Information System covered by the regulation. Qualifying licensees need only comply with a subset of the §500.19(a) exemption applicable requirements.

For a list of applicable regulation requirements by exemption status, please see **here**. Exemptions do not expire and do not need to be filed again once an initial filing has been made. However, a fresh filing is required for any changes to exemption status. Data and documentation supporting the filing of an exemption should be retained for five years.

CERTIFICATION OF COMPLIANCE FILING (See §500.17(b) of the regulation) — APPLIES TO §500.19(a)/(c) EXEMPTS

Licensees must file an annual Certification of Compliance with the DFS by April 15th of every year attesting to **full compliance** with the requirements of the regulation that were applicable to the licensee during the preceding year. Please see **here** for filing instructions. Individuals with a **§500.19(b)** exemption do not need to certify. Certifications should be filed on the DFS' cybersecurity **web portal** between January 1st and April 15th (do not file prior to January 1st). Submission of supporting documentation is not required but should be maintained by the licensee in case the DFS requests such information in the future. The Chair of the Board of Directors or a Senior Officer(s) of the licensee must execute the Certification[4]. To the extent a licensee has identified areas, systems or processes that require material improvement, updating or redesigning, the licensee must document the identification and remedial efforts, both planned and underway, to address such areas, systems or processes. Documentation must be available for inspection by the Superintendent of Financial Services and all records, schedules and data supporting the certification must be maintained for a period of five years.

CYBERSECURITY PROGRAM (See §500.02 of the regulation) — APPLIES TO NONEXEMPTS AND §500.19(a) EXEMPTS

Licensees must maintain a Cybersecurity Program that is based on a licensee's Risk Assessment (discussed later) and must be focused on identifying, preventing, detecting, responding to, recovering from and reporting Cybersecurity Events[5]. A licensee may adopt all or part of an Affiliate's program regardless of whether that Affiliate is subject to the regulation. However, the licensee will be held fully responsible for all

---

[2] "Information Systems" is broadly defined and includes any electronic system that collects, processes, maintains, uses, shares, disseminates or disposes of electronic information. A broker management system or email system come under this definition.

[3] "Nonpublic Information" is defined as all electronic information that is not publicly available and is:

- Business related information that if tampered with or breached could, or did in fact, cause a material adverse impact on the licensee
- Information about a third-party that combines a name, number, or other identifier with one of the following:
  - Social Security number
  - Driver's license or non-driver ID card
  - Account number, credit or debit card number
  - Security code, access code or password that permits access to an individual's financial account
  - Biometric records
- Health or health care information, payment for the provision of health care information

[4] The Big I New York has received instruction from the DFS that LLCs, which typically have neither a Board nor Senior Officers, should look to the definition of a "Senior Officer(s)" as "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." Such an individual(s) should execute the Certification and select the "Senior Officer(s)" checkbox.

[5] A "Cybersecurity Event" is any attempt, whether successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on that system.

elements of its Program. The DFS has **stated** its expectations when a licensee adopts an Affiliate's practices. All information related to a Program must be made available to the New York Superintendent of Financial Services upon request.

CYBERSECURITY POLICY (See §500.03 of the regulation) — APPLIES TO NONEXEMPTS AND §500.19(a) EXEMPTS

Licensees must have a written Cybersecurity Policy that is approved by a Senior Officer, the Board of Directors, a committee of the Board or an equivalent governing body. The Policy must be based on the licensee's Risk Assessment and document how the licensee intends to protect its Information Systems and any Nonpublic Information stored on those systems. The regulation specifies 14 areas that must be addressed to the extent possible.

CHIEF INFORMATION SECURITY OFFICER (See §500.04 of the regulation) — APPLIES TO NONEXEMPTS

Each licensee must designate a "qualified" (undefined term) Chief Information Security Officer (CISO) to implement and oversee the licensee's Cybersecurity Program and to enforce its Cybersecurity Policy. The CISO can be a third-party provider or an employee of an affiliate. ELANY recommends that exempt licensees appoint a responsible qualified individual to oversee their cybersecurity efforts even though this requirement does not apply to them under the regulation.

The CISO must report at least annually to the licensee's full Board of Directors (not a committee) or an equivalent body on the status of the Program and material risks. If there is no Board or equivalent body, the report must be made to a Senior Officer who is responsible for the licensee's Cybersecurity Program.

PENETRATION TESTING AND VULNERABILITY ASSESSMENT (See §500.05 of the regulation) — APPLIES TO NONEXEMPTS

A Cybersecurity Program must include monitoring and testing which is developed in accordance with the licensee's Risk Assessment and incorporates continuous monitoring or other systems that detect vulnerabilities on a continuous basis. Manual periodic reviews of logs and firewall configurations do not qualify. In the event continuous monitoring or other similar protocols are not available, licensees must conduct annual penetration testing based on the Risk Assessment AND bi-annual vulnerability assessments, such as scans, that are designed to identify cybersecurity vulnerabilities.

AUDIT TRAIL (See §500.06 of the regulation) — APPLIES TO NONEXEMPTS

Each licensee must ensure, based on its Risk Assessment, that it can reconstruct material financial transactions sufficient to support normal operations. In addition, the licensee must put in place audit trails that can detect and respond to Cybersecurity Events that have a reasonable chance of harming any material part of the licensee's normal business operations.

ACCESS PRIVILEGES (See §500.07 of the regulation) — APPLIES TO NONEXEMPTS AND §500.19(a) EXEMPTS

A licensee's Cybersecurity Program must limit user access privileges to Information Systems that contain Nonpublic Information. This action must be based on the licensee's Risk Assessment and access privileges must be reviewed periodically.

APPLICATION SECURITY (See §500.08 of the regulation) — APPLIES TO NONEXEMPTS

Cybersecurity Programs must include written procedures, guidelines and standards to ensure the secure development of applications that are developed in-house and for assessing the security of externally developed applications. These procedures, guidelines and standards must be periodically reviewed, assessed and updated as necessary by the Chief Information Security Officer or a qualified designee.

RISK ASSESSMENT (See §500.09 of the regulation) — APPLIES TO NONEXEMPTS AND §500.19(a)/(c) EXEMPTS

Each licensee must conduct a periodic Risk Assessment of its Information Systems that can be used to develop its Cybersecurity Program. The Risk Assessment must consider the licensee's particular cybersecurity risks to the extent they may impact Nonpublic Information and Information Systems, and must be updated as relevant changes occur.

CYBERSECURITY PERSONNEL AND INTELLIGENCE (See §500.10 of the regulation) — APPLIES TO NONEXEMPTS

Each licensee must utilize "qualified" (undefined term) cybersecurity personnel to manage the licensee's cybersecurity risks and to perform, or oversee, the core cybersecurity functions specified by its Cybersecurity Program. Such personnel must be provided with training and updates sufficient to deal with relevant cybersecurity risks. In addition, the licensee must verify that key cybersecurity personnel take steps to maintain knowledge of changing threats and countermeasures.

THIRD-PARTY SERVICE PROVIDER SECURITY POLICY (See §500.11 of the regulation) — APPLIES TO NONEXEMPTS AND §500.19(a)/(c) EXEMPTS

Licensees must implement written policies to ensure the security of Nonpublic Information and Information Security Systems that are accessible by Third-Party Service Providers.[6] Policies must reflect the licensee's Risk Assessment. Licensees must perform due diligence to ensure the adequacy of Third-Party Service Providers, but sole reliance on a Third-Party Service Provider's own Certification of Compliance does not constitute adequate due diligence.

A producer, employee, representative or designee of a licensee need not have his or her own Third-Party Service Provider policy if they follow the policy of the licensee.

MULTI-FACTOR AUTHENTICATION (See §500.12 of the regulation) — APPLIES TO NONEXEMPTS

A licensee must institute controls that are based on its Risk Assessment, which may include multi-factor authentication (password + email/text code, etc.) or risk-based authentication, to protect Nonpublic Information and Information Systems. Unless the Chief Information Security Officer authorizes an alternative system that offers equivalent or greater security, multi-factor authentication must be used for anyone entering the licensee's internal network from an external network. Internal networks include email, document hosting and related services whether on-premises or in the cloud. The DFS views multi-factor authentication as essential and has provided **guidance** on its views and expectations.

LIMITATIONS ON DATA RETENTION (See §500.13 of the regulation) — APPLIES TO NONEXEMPTS AND §500.19(a)/(c) EXEMPTS

Each licensee must, as part of its Cybersecurity Program, have policies and procedures for the periodic disposal of Nonpublic Information that is no longer necessary for business operations or other business purposes, subject to applicable record retention requirements. This requirement does not apply where disposal is not feasible due to the manner in which the information is maintained.

[6] The regulation defines a "Third Party Service Provider" as a person or non-governmental entity that is not an affiliate of the licensee, provides services to the licensee and is permitted to access Nonpublic Information as part of providing services to the licensees.

TRAINING AND MONITORING (See §500.14 of the regulation) — APPLIES TO NONEXEMPTS

As part of its Cybersecurity Program, a licensee must have policies, procedures and controls in place to both monitor the activity of authorized Information System users and detect unauthorized access or tampering with Nonpublic Information by authorized users. In addition, a licensee must provide regular cybersecurity awareness training for all personnel that is updated to reflect the licensee's Risk Assessment. The regulation does not define acceptable training but ELANY suggests that it include elements such as how to protect against phishing emails, CEO fraud and ransomware, as well as protecting passwords.

ENCRYPTION OF NONPUBLIC INFORMATION (See §500.15 of the regulation) — APPLIES TO NONEXEMPTS

Each licensee's Cybersecurity Program must implement controls based on its Risk Assessment, including encryption, to protect Nonpublic Information both in transit via external networks and at rest. If encryption of Nonpublic Information is deemed by the licensee to be infeasible, the Chief Information Security Officer may authorize other controls.

INCIDENT RESPONSE PLAN (See §500.16 of the regulation) — APPLIES TO NONEXEMPTS

A licensee must establish an incident response plan as part of its Cybersecurity Program to respond to Cybersecurity Events that materially impact the confidentiality, integrity or availability of the licensee's Information Systems or any part of its business.

The plan must address processes, goals, roles, communication, identification and remediation of control weaknesses, reporting and documentation, and evaluation of the plan following a Cybersecurity Event.

NOTICES TO SUPERINTENDENT (See §500.17(a) of the regulation) — APPLIES TO NONEXEMPTS AND §500.19(a)/(c) EXEMPTS

Licensees must notify the Superintendent of Financial Services within 72 hours following a determination that a Cybersecurity Event has occurred if notice is required to any government body, self-regulatory agency or any other supervisory body (i.e., NYS Information Security Breach and Notification Act) OR the Cybersecurity Event has a reasonable likelihood of materially harming any material part of the covered entity's normal operations. A Cybersecurity Event that involves harm to consumers must be reported. A licensee must directly report a Cybersecurity Event to the DFS even if a Third Party Service Provider does so or offers to do so. The DFS requests that licensees notify the Department regarding unsuccessful attacks that appear particularly significant based on the Covered Entity's understanding of the risks it faces. The DFS has stated that it does not intend to penalize licensees for honest, good faith reporting judgments. Reporting should be done via the **DFS portal**.

The DFS refers small licensees to the Global Cyber Alliance Toolkit for Small Business "to help small businesses improve their cybersecurity." Use of these specific policy documents is at the discretion of the licensee.

120 Wall Street, 24th Floor
New York, NY, 10005
(646) 292-5500
elany@elany.org | www.elany.org

This advisor is not intended to be nor should it be construed as legal advice. These guidelines are provided for your consideration and for use in consultation with your legal counsel.