PROFESSIONAL INSURANCE AGENTS

April 2021

New York's cybersecurity regulation in a nutshell—*23 NYCRR 500*

WHO NEEDS TO COMPLY?

All insurance agents, brokers and companies that are licensed in New York state are subject to the requirements of this regulation. This includes nonresident licensees. **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*."

A LOOK BACK: WHEN DID I NEED TO COMPLY BY?

The effective date of the new regulation was March 1, 2017.

You had 180 days, or until Aug. 28, 2017, to become compliant. Additionally, there are phase-in transition periods for the different provisions. So, the earliest that you had to comply with any part of the regulation was Aug. 28, 2017.

- **On or before Sept. 27, 2017 (was extended to Oct. 30, 2017)—initial 30-day period for filing Notices of Exemption.**
- **On or before Feb. 15, 2018—the first annual certification of compliance was due to the New York State Department of Financial Services.**

WHAT DO I NEED TO DO?

—First, send in your certifications

Send the following two certification forms to NYDFS:

1. **File your LIMITED EXEMPTION FORM via the DFS secure portal:** http://on.ny.gov/2qTdBPR .

   You will first be prompted to Create an Account at the bottom of the screen on the secure portal. This account and portal will be used for future regulatory filings relating to cybersecurity, including notices of cybersecurity events and certifications of compliance.

   Then follow the following steps:

   1. Enter your name and email address (start with your agency name, although you will need to do this for all of your licenses (individual and business entity). Don't forget the Text Verification on the right-hand side of the form.

2. Hit Submit, and a temporary Password will be emailed to you.
3. Open your email and log on with that password. This will prompt you to Change your Password.
4. Click on the link: "If you are looking to submit your cybersecurity regulations, please click below: https://myportal.dfs.ny.gov/web/cybersecurity."
5. You will see three boxes. Choose the box to the RIGHT, titled "Submit Cybersecurity Notice of Exemption."
6. Enter your Entity I.D. (license number) or name. Use the name of your agency, the name of your individual license and your New York state license number. (Give it a minute as it searches for your license). Choose the appropriate license and select it on the drop-down menu.
7. Click Next.
8. You will have an opportunity to choose the reasons for your exemption:
    a. For agencies, you should select all that apply:
        i. Section 500.19(a)(1—less than 10 employees
        ii. Section 500.19(a)(2)—less than $5 million in revenue
        iii. Section 500.19(a)(3)—less than $10 million in assets
    b. For individual licenses, you should choose
        i. Section 500.19(b)—"employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity."
9. Hit Next.
10. Enter your Contact information, click the box and hit Submit.
11. You will then get an Acknowledgement. Print this acknowledgement and put it in your cybersecurity files.

The department reminds Covered Entities that Notices of Exemption should be filed electronically via the DFS Web Portal.

What is the limited exemption? The limited exemption applies to covered entities with:

- **fewer than 10 employees** (part-time or full-time), including any independent contractors, of the covered entity or its affiliates located in New York or responsible for business of the covered entity, or
- **less than $5,000,000 in gross annual revenue** in each of the last three fiscal years from New York business operations of the covered entity and its affiliates, or
- **less than $10,000,000 in year-end total assets,** calculated in accordance with generally accepted accounting principles, including assets of all affiliates.

Only one of the above-noted items needs to be met to meet the limited exemption.

2. **After you've completed your compliance documents below, send in your CERTIFICATION OF COMPLIANCE FORM which is due each April 15 for the prior year, via the DFS secure portal:** http://on.ny.gov/2qTdBPR. A Covered Entity may not submit a certification under 23 NYCRR 500.17(b) unless the Covered Entity is in compliance with all applicable requirements of Part 500 at the time of certification.

The board of directors or a senior officer(s) of the Covered Entity certifies:

1. *the board of directors (or name of senior officer(s) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary; and*
2. *to the best of the (board of directors) or (name of senior officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of (date of the board resolution or senior officer(s) compliance finding) for the year ended (year for which board resolution or compliance finding is provided) complies with Part 23 NYCRR 500.*

_____

Signed by the chairperson of the board of directors or senior officer(s)

—Next, prepare your compliance documents

Fill in the following paperwork and keep copies for your files (*DO NOT send to DFSDFS*):

1. **CONDUCT A RISK ASSESSMENT of your information system *(computers)*:**
https://www.pia.org/IRC/askpia/show.php?apid=310411
The Risk Assessment must be carried out in accordance with written policies and procedures and must be documented. Such policies and procedures must include:
    1. criteria for the **evaluation and categorization of identified cybersecurity risks or threats facing your information system**;
    2. criteria for the **assessment of the confidentiality, integrity, security and availability of your information systems and nonpublic information,** including the adequacy of existing controls in the context of identified risks; and
    3. requirements describing **how identified risks will be mitigated** or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

    Use the following risk mitigation operation checklist to complete your risk assessment:
    - Create a hardware, software and information systems inventory.
    - Determine how the loss or short-term unavailability of data might impact operations.
    - Update and test data backup, recovery and contingency procedures.
    - Ensure that password access on computers coincides with the level of actual access needed by any given employee based upon job description.
    - Establish detailed password guidelines, specifying password length and acceptable configuration and requiring periodic password changes and other protection protocol.
    - Reposition computer monitors and apply automatic log-out mechanisms to assure systems security.
    - Install virus-scanning software on all relevant devices on and offsite.
    - Conduct phishing campaigns to test the susceptibility of personnel to click on suspicious links that can result in system infiltration.
    - Scrutinize offsite access of computer networks, including the efficacy of identity authentication steps, and the proper use of storage media and nonsecured personal telephone and mobile devices for work activities.
    - Create forms to document investigation, mitigation and resolution of security incidents.
    - Provide formal risk assessment and cybersecurity training and alert personnel that they are subject to administrative monitoring, thus eliminating any expectation of privacy.
    - Execute agreements contemplating vendor and third-party security breaches.
    - Provide detailed instructions regarding the reporting and documentation of security breaches, including to whom such breaches should be reported—governmental authorities or otherwise.
    - Produce an audit log of excessive or unusual systems activity.
    - Require that all lost or stolen access devices such as cards and keys, company laptops or mobile devices be reported.

2. **PREPARE A CYBERSECURITY PROGRAM:**
You are required to maintain a cybersecurity program in your agency designed to protect the confidentiality, integrity and availability of your information systems.

    Your cybersecurity program will be *based on the results of your risk assessment (above)* and designed to perform the following core cybersecurity functions:

    I. identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on your information systems *(use checklist above)*;
    II. use defensive infrastructure and the implementation of policies and procedures to protect your information systems, and the nonpublic information stored on those

information systems, from unauthorized access, use or other malicious acts *(antivirus and firewall, secure computers at night, regularly change passwords, restrict access to data and systems)*;

III. detect cybersecurity events *(antivirus and firewall)*;
IV. respond to identified or detected cybersecurity events to mitigate any negative effects *(antivirus and firewall)*;
V. recover from cybersecurity events and restore normal operations and services *(antivirus and firewall)*; and
VI. fulfill applicable regulatory reporting obligations *(use DFS secure portal to report cybersecurity events)*.

3. PREPARE A WRITTEN CYBERSECURITY POLICY:

You need to implement and maintain a **written policy** or policies in your agency setting forth ***your policies and procedures for the protection of your information systems*** and the Nonpublic Information stored on those information systems.

Like the cybersecurity program, your cybersecurity policy will be ***based on your risk assessment*** and needs to address the following areas:

I. information security *(antivirus and firewall, passwords);*
II. data governance and classification *(what types of data do you store and where);*
III. asset inventory and device management *(physical count of computers);*
IV. access controls and identity management *(passwords and who has access);*
V. business continuity and disaster-recovery planning and resources *(backups);*
VI. systems operations and availability concerns *(procedures if you are hacked);*
VII. systems and network security *(antivirus and firewall);*
VIII. systems and network monitoring *(antivirus and firewall);*
IX. systems and application development and quality assurance *(antivirus and firewall);*
X. physical security and environmental controls *(locked doors, logging off at night);*
XI. customer data privacy *(require passwords);*
XII. vendor and third-party service provider management *(assurances that your partners are secure);*
XIII. risk assessment *(above);* and
XIV. incident response *(above).*

HOW TO FILE CYBERSECURITY EVENT NOTICES

Covered Entities are required to notify the superintendent of cybersecurity events as promptly as possible, but in no event later than 72 hours from a determination that a reportable Cybersecurity Event has occurred. At this time, covered entities should send all notices of cybersecurity events to your normal supervisory staff within the department. The DFS web portal will accommodate notices of cybersecurity events and certifications of compliance shortly. See: https://www.dfs.ny.gov/industry_guidance/cyber_faqs.
So, send your forms to:

New York State Department of Financial Services
One State St.
New York, NY 10004-1511

And send them with a proof of mailing and keep copies in your files!

YOU ALSO MUST:

1. Limit and periodically review access privileges to your information system (*who can log onto your computers*).
2. Provide notice to the superintendent of a cybersecurity event, if one occurs (*see above*). Use this NYS Security Breach Reporting Form.
   A **THIRD-PARTY PROVIDER SECURITY POLICY,** has been required since March 2019.

   - 23 NYCRR 500.11 generally requires a Covered Entity to develop and implement written policies and procedures designed to ensure the security of the Covered Entity's Information Systems and Nonpublic Information that are accessible to, or held by, Third- Party Service Providers.

WHERE CAN I GET SOME HELP WITH THIS?

PIA offers its Privacy Compliance Central tool kit with access to a library of information on this regulation at: https://www.pia.org/IRC/privacy/#cyber.
Additionally, a local vendor, *TAG Solutions* offers PIA members two programs to help member agencies become compliant with these new rules:

- **Compliance Plus,** allows agencies to not just simply comply, but to fully secure their information systems; or
- **Do-It-Yourself,** which offers agencies sample cybersecurity forms that they can fill in themselves for compliance.

Find more information here.

4/21
Think PIA first