CITRINCOOPERMAN®
FOCUS ON WHAT COUNTS

WWW.CITRINCOOPERMAN.COM

MANDATORY NYS CYBERSECURITY REGULATIONS FOR FINANCIAL SERVICES COMPANIES - SUMMARY*

All financial services entities (banks, insurance companies and agents, financial services, etc.) that are regulated, licensed, or supervised by the New York State Department of Financial Services (NYS DFS) are required to comply with new mandatory cybersecurity requirements in New York's Cybersecurity Regulation: 23 NYCRR Part 500.

1 DOES THE 23 NYCRR PART 500 CYBERSECURITY REGULATIONS APPLY TO YOU?

Use this link: http://www.dfs.ny.gov/about/whowesupervise.htm to quickly determine if your organization is listed in the NYS DFS database. All listed and "covered entities" need to comply with the mandatory cybersecurity regulations detailed in 23 NYCRR Part 500. Even entities not listed or required to adhere to the NYS DFS regulations should still be aware of the risks posed by cybersecurity to their business and be actively developing internal strategies for protection and prevention.

2 WHICH SET OF MANDATORY REQUIREMENTS MUST YOU COMPLY WITH?

If you are a "covered entity" you must comply with one of the 2 sets of regulations below and provide annual proof of compliance. Please check to see which set applies to you: the full set or the smaller set based on meeting certain exemptions:

FULL SET OF MANDATORY REGULATIONS

- Maintain a Cybersecurity Program
- Implement Written Cybersecurity Policies
- Designate a CISO (Chief Information Security Officer)
- Perform Penetration Testing & Vulnerability Assessments
- Maintain Systems for Audit Trails
- Control & Manage Access Privileges
- Application Security Procedures and Testing
- Perform Periodic Risk Assessments
- Utilize Qualified Cybersecurity Personnel & Intelligence
- Maintain Third Party Service Provider Security Policies
- Employ Multi-Factor Authentication
- Develop Procedures for Data Retention & Data Disposal
- Perform Activity and Access Monitoring
- Conduct Regular Cybersecurity Awareness Training
- Control and Encrypt Data
- Create a Written Cybersecurity Incident Response Plan
- Provide Notifications of Cybersecurity Events to the Superintendent (NYS DFS)
- Prepare & Submit Annually a Certification of Compliance

DO THE FOLLOWING LIMITING EXEMPTIONS APPLY TO YOU?

- Entities with fewer than 10 employees, including independent contractors, or
- Entities with less than $5 million in gross annual revenue in each of the last three fiscal years, or
- Entities with less than $10 million in year-end total assets, including assets of all affiliates

MANDATORY REGULATIONS FOR LIMITED EXEMPTION ENTITIES

- Maintain a Cybersecurity Program
- Implement Written Cybersecurity Policies
- Control & Manage Access Privileges
- Perform Periodic Risk Assessments
- Maintain Third Party Service Provider Security Policies
- Develop Procedures for Data Retention & Data Disposal
- Provide Notifications of Cybersecurity Events to the Superintendent (NYS DFS)
- Prepare & Submit Annually a Certification of Compliance

3 KEY DATES UNDER NEW YORK'S CYBERSECURITY REGULATION (23 NYCRR PART 500)

March 1, 2017	**Effective Date** - NYS Cybersecurity Regulations became effective (23 NYCRR Part 500)
August 28, 2017	**Deadline for Compliance** - Covered Entities are required to be in compliance with the requirements of 23 NYCRR Part 500, unless otherwise specified
September 27, 2017	**Deadline for Exemption Notice** - Covered Entities that qualify for a limited exemption must file a Notice of Exemption by this date.
February 15, 2018	**Deadline for 1st Annual Certification Submission** - Covered Entities are required to file their 1st Certification of Compliance by this date.
March 1, 2018	**1 Year Transitional Period Ends** - Covered Entities are required to be in compliance with the requirements of section 500.04(b), 500.05, 500.09, 500.12, and 500.14(b) of 23 NYCRR Part 500 (see regulations document for details of the sections above)
September 3, 2018	**18 Month Transitional Period Ends** - Covered Entities are required to be in compliance with the requirements of section 500.06, 500.08, 500.13, 500.14(a), and 500.15 of 23 NYCRR Part 500 (see regulations document for details of the sections above)
February 15, 2019	**Deadline for 2nd Annual Certification Submission** - Covered Entities are required to file their 2nd Certification of Compliance by this date.
March 1, 2019	**Deadline for Full Compliance for All** - Covered Entities are required to be fully compliant with the requirements of 23 NYCRR Part 500

4 NEED HELP DEALING WITH CYBERSECURITY AND THE NYS DFS REGULATIONS?

Understanding cybersecurity policies and procedures, how these new regulations apply to you, and how much work it will require to become compliant can all be very confusing and overwhelming. To simplify this process, Citrin Cooperman has developed some simple and intuitive tools to help you reliably assess and understand where you are in this process. Once you have determined your status, our experts can then help you to create a strategy which includes plans, procedures, timelines and processes to meet the necessary regulations, become compliant and most of all to help keep your business and data secure. Contact us today for questions or assistance.

+1 914.693.7000 trac@citrincooperman.com citrincooperman.com

** - This document was prepared by Citrin Cooperman to summarize the requirements of 23 NYCRR 500 in a condensed version. It does not include all language, provisions, requirements and/or regulations of the actual NYS document. Please be sure to download and review the full document from http://www.dfs.ny.gov/.*