# SAGE SOLUTIONS BRIEF

# New York Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500)

sage
DATA SECURITY

PROTECTING INFORMATION ASSETS | ENSURING REGULATORY COMPLIANCE | FIGHTING CYBERCRIME

# Table of Contents

## About 23 NYCRR 500

In response to the ever-growing threat of cyber-attacks, the New York State Department of Financial Services (NYSDFS) issued 23 NYCRR 500, which outlines cybersecurity requirements and regulatory minimum standards for financial services companies. It applies to any company subject to the authority of NYSDFS under New York banking, insurance, and financial services law.

The Rule went into effect on March 1, 2017. It is divided into 16 sections, seven of which must be completed by the end of August 2017. The others have start dates of one year, 18 months, or two years. The message is clear though. All Covered Entities must make cybersecurity a priority, and “move swiftly and urgently to adopt a cybersecurity program” as outlined in the regulation.

The core of the cybersecurity regulation is developing a robust **risk-based cybersecurity program** that protects the confidentiality, integrity, and availability of nonpublic data. The program must be overseen and enforced by a qualified **Chief Information Security Officer (CISO)**, who can either be an in-house employee or a third-party resource.

The Program should:

1. Identify and assess the cybersecurity risks that threaten data security or integrity, both internal and external.
2. Implement infrastructure, policies, and procedures, so that when an organization experiences a cybersecurity event, they can detect it, respond to it, recover from it, and then report it appropriately.

## How Sage Can Help

The new regulations are not prescriptive in nature. There isn’t a one-size-fits-all approach. Instead, the requirements are tied to the institution’s risk assessment. This provides flexibility, but also puts the onus on the institution to determine what an “acceptable level” of risk is for their business.

At Sage, we understand that cybersecurity isn’t a one-size-fits-all proposition. We’ve been working with financial services companies for nearly two decades helping them to identify and assess risk and vulnerabilities, detect cybersecurity events, and respond to and recover from incidents. We believe that information security is more than a compliance obligation. It's a commitment to honor those who have entrusted you with their information assets. It is a shared responsibility and a civic duty.

Sage advisors and analysts operate as an extension of your team. We don’t sell any third-party hardware or software, and we don’t endorse or represent any vendor. We’re experts who you can communicate with on the phone, over email, or in person about your questions and concerns. We aren’t satisfied with our job until we’ve made sure that you are completely comfortable and confident in the cybersecurity plan of action we’ve developed together.

Keep reading to explore how Sage can help you comply with 23 NYCRR 500 or contact us (207-879-7243) for more information!

## *Section 500.02 Cybersecurity Program*

Establish a risk-based cybersecurity program designed to protect information systems and nonpublic information; detect, respond to, and recover from cyber events; and fulfill all reporting obligations.

- Sage's **Program Development and Advisory Services** can support program, policy and procedure development and assessment across enterprise control categories including Program Governance, Continuity of Operations / Disaster Recovery, Incident Response, and Risk Management.

- Ongoing monitoring, analysis, and detection of cybersecurity events is provided by Sage's ***n*Discovery Managed Threat Detection Service**. Combining human expertise with the latest threat intelligence and advanced data analytics, we quickly and accurately detect threats across your entire environment. We validate the breadth of an incident and deliver remediation recommendations to you within minutes.

- Prepare your incident responders and IT personnel to quickly and cost-effectively capture and maintain evidence in a forensically sound manner with Sage's **Cyber Forensics Readiness Program**. Or we can facilitate a **Cyber Incident Response Exercise** to allow your entire incident response team to practice and refine their skills.

## *Section 500.03 Cybersecurity Policy*

Create and maintain written policies and procedures for the protection of information systems and nonpublic information based on the company's risk assessment.

- Sage's **Information Security Policy Development & Assessment** will review existing policies for compliance with best practices and legal requirements. We will make the necessary updates to ensure the resulting policy set satisfies regulatory expectations. Sage's methodology for policy and standards development is collaborative. We work with management and staff to incorporate existing documents and practices, as well as develop new policies, standards, and agreements.

## *Section 500.04 Chief Information Security Officer*

Designate a qualified Chief Information Security Officer (CISO) to oversee the cybersecurity program. It can be either an in-house employee or a third-party service provider.

- Sage's **Cybersecurity Partnership Program** provides oversight, guidance, and counsel toward meeting compliance objectives and improving the security posture throughout your organization. The annual subscription program provides you access to a dedicated Sage expert, plus keeps you up-to-date on the latest cybersecurity updates and best practices through monthly webinars. The Program includes regularly scheduled on-site meetings where your advisor will provide guidance on cybersecurity initiatives.

## *Section 500.05 Penetration Testing and Vulnerability Assessments*

Include monitoring and testing designed to assess the effectiveness of the cybersecurity program.

- At Sage, our network **Penetration Tests and Vulnerability Assessments** are more than just running an automated scan. We have over a decade of experience tailoring tests to your specific environment, and deliver concise, actionable findings and effective remediation recommendations.

- Sage's **Social Engineering Vulnerability Assessments** can help you track the success of your training programs and determine additional training needs. Our assessments will identify and document successes and failures in user interaction with information systems, observance of confidentiality practices and procedures, as well as incident recognition, reporting, and response.

## *Section 500.06 Audit Trail*

Securely maintain a system that can reconstruct material financial transactions following an event, and audit trails to detect and respond to cybersecurity events.

- Sage's ***n*****Discovery Managed Threat Detection Service** collects and stores event logs across your entire network environment. If a unique or suspicious event is identified, we have access to forensic-quality data to research and confirm the legitimacy of an event. If an incident is confirmed, you are notified immediately with the exact details of what happened, which files are affected, and what you should do about it.

## *Section 500.07 Access Privileges*

Limit user access privileges to systems that provide access to nonpublic information, with periodic review of such privileges.

- Sage's ***n*****Discovery Managed Threat Detection Service** monitors and reports out on all administrative and user activity every day, providing oversight of system access privileges.

## *Section 500.08 Application Security*

Include written procedures, guidelines, and standards within your cybersecurity program that ensure the use of secure development practices for in-house developed applications.

- Sage's **Information Security Policy Development & Assessment** includes assessment and recommendations in a variety of areas, including guidelines for in-house developed applications.

## *Section 500.09 Risk Assessment*

Conduct periodic risk assessment of information systems to inform the design of the cybersecurity program.

- Sage's **Risk Management Framework Development** determines the relative significance of your assets, so you can determine the frequency by which they should be scrutinized for risk exposures. We work collaboratively with you to develop an operational framework that is optimized for the size, scope, and complexity of your business.

- Sage's **Information Security Risk Assessment** identifies the criticality and sensitivity of information and corresponding information systems, the potential exposure from threats and vulnerabilities, and the adequacy of mitigating and compensating controls. Risk assessments for regulated organizations should focus on both the risk to the organizational information as well as regulatory protected data.

## *Section 500.10 Cybersecurity Personnel and Intelligence*

Utilize qualified cybersecurity personnel (or a third-party service provider) to manage the organization's risk and to perform or oversee the performance of the core cybersecurity functions. Provide training and resources, so personnel can maintain current knowledge of changing cybersecurity threats and countermeasures.

- Sage's **Cybersecurity Partnership Program** provides oversight, guidance, and counsel toward meeting compliance objectives and improving the security posture throughout the organization. The annual subscription program provides you access to a dedicated Sage expert, plus keeps you up-to-date on the latest cybersecurity updates and best practices through monthly webinars. The Program includes regularly scheduled on-site meetings where your advisor will provide guidance on cybersecurity initiatives.

- As a subscriber to Sage's ***n*Discovery Managed Threat Detection Service**, you have access to a Threat Intelligence Center which provides data on recent malware detected, including IP address and origin.

## *Section 500.11 Third-Party Service Provider Security Policy*

Implement written policies and procures to ensure the security of information systems and nonpublic information accessible by third-party service providers.

- Sage's **Service Provider Cybersecurity Assessment Program** supports the management of all your third-party service providers and ensures you are in compliance with 23 NYCRR 500, utilizing the most recent FFIEC guidance provided by Appendix J of the FFIEC Business Continuity IT Handbook. We'll work with you to set-up your program, collect documentation, and then perform a cybersecurity review.

## *Section 500.12 Multi-Factor Authentication*

Utilize effective controls to protect against unauthorized access to nonpublic information or information systems, and multi-factor authentication is required for accessing your internal network from an external network.

- Sage's **IT Infrastructure Risk Assessment** looks at the design, configuration, and operational processes that are critical to your information technology infrastructure. We identify the inherent risks (operational, reputational, strategic, compliance, transactional), of probable threats, assess current protections, and determine residual risk levels. If our assessment determines your IT infrastructure is at undue risk, we will recommend specific mitigation strategies. As part of this process we will identify and enumerate those systems that are subject to this requirement.

## *Section 500.13 Limitations of Data Retention*

Include policies and procedures for the secure disposal on a periodic basis for nonpublic information.

- Sage's **Information Security Policy Development & Assessment** includes assessment and recommendations in a variety of areas, including guidelines for data retention and secure disposal.

## *Section 500.14 Training and Monitoring*

Implement policies, procedures, and controls designed to monitor activity of Authorized Users, and detect unauthorized access of, use of, or tampering with nonpublic data by such Authorized Users.

- As a subscriber to Sage's ***n*Discovery Managed Threat Detection Service** you receive daily reports, as well as real-time alerts of all administrative activity.  Any unauthorized access of, use of, or tampering with protected data is detected within minutes.

Provide regular cybersecurity awareness training.

- Sage offers a variety of targeted **Cybersecurity Awareness Training** sessions for employees. Whether you're looking to give your staff concise, practical training that will help them implement best practices and follow company policy, or to simply increase the cybersecurity awareness of your employees or client base, your company will benefit from our training.

## *Section 500.15 Encryption of Nonpublic Information*

Implement controls, including encryption, to protect nonpublic information held or transmitted. When encryption isn't feasible, compensating controls reviewed and approved by the CISO may be used.

- Sage's **IT Infrastructure Risk Assessment** includes recommendations for specific risk mitigation strategies and controls, including encryption, and provides guidance for reasonable compensating controls.

## *Section 500.16 Incident Response Plan*

Establish a written incident response plan designed to promptly respond to, and recover from, a cybersecurity event.

- Sage's security experts can work with you to develop an **Incident Response Plan** that will ensure the sustainability and success of your organization when faced with the uncertainty that accompanies incidents ranging from cases of innocuous mistaken identity to sophisticated and complex cyber-attacks.

- Sage offers two types of **Cyber Incident Response Exercises**. The first is an *Incident Preparedness* exercise designed to start the right conversations and planning initiatives. The second is a *Plan Evaluation* exercise designed to put your Incident Response Plan to the test and identify opportunities for improvement.

## *Section 500.17 Notices to Superintendent*

A cybersecurity event must be reported to the superintendent no later than 72 hours from detection.

- As part of Sage's **Incident Response Plan Development** we can develop a satisfactory template to meet these requirements.

## *Section 500.18 Confidentiality*

Information provided by a Covered Entity is subject to exemptions from disclosure under the applicable state or federal law.

- Sage's team of security professionals are credentialed by internationally recognized organizations such as ISC$^2$ and ISACA. In addition, they have years of experience working in the information security industry. All Sage employees undergo extensive background checks. All Sage engagements are conducted within applicable confidentiality regulations.

## *Section 500.19 Exemptions*

Limited exemptions are available for requirements set in section 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16.

- Sage works with organizations of all sizes. Each engagement is tailored based on the size and scope of the organization's infrastructure.

## *Section 500.20 Enforcement*

This regulation will be enforced by the superintendent, and is not intended to limit authority under any applicable laws.

- Sage will provide guidance, counsel, and advice for relevant enforcement guidelines.

## *Section 500.21 Effective Date*

Effective March 1, 2017, a senior officer must review all documentation and sign a certification of compliance on an annual basis starting on February 15, 2018. This means executives have to be an active part of the cybersecurity conversation.

- Sage's **Executive Cybersecurity Readiness Program** can help you keep Executives and Boards of Directors up-to-date on the latest cybersecurity landscape. The program includes an onsite Board briefing, quarterly webinars, a cybersecurity resilience assessment, and a cyber incident response exercise.

## *Section 500.22 Transitional Periods*

Covered entities have 180 days from the effective date to comply with many of the requirements of this regulations. Other requirements offer additional transitional periods of one year, 18 months, or two years.

- Partnering with Sage in 2017 will ensure compliance with the February 15, 2018, deadline.

Download 23 NYCRR 500 at the NYSDFS's website - www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

**Learn more at www.sagedatasecurity.com/23-nycrr-500-compliance**

## Sage Solution Matrix

| 23 NYCRR 500 Section | Sage Solution |
|---|---|
| Section 500.02 Cybersecurity Program | • Information Security Policy Development & Assessment<br>• Disaster Recovery Program Development<br>• Incident Response Plan Development<br>• nDiscovery Managed Threat Detection Service<br>• Cyber Forensics Readiness Program<br>• Cyber Incident Response Exercise |
| Section 500.03 Cybersecurity Policy | • Information Security Policy Development & Assessment |
| Section 500.04 Chief Information Security Officer | • Cybersecurity Partnership Program |
| Section 500.05 Penetration Testing and Vulnerability Assessments | • Network Penetration Tests (External, Internal, Web App)<br>• Vulnerability Assessments<br>• Social Engineering |
| Section 500.06 Audit Trail | • nDiscovery Managed Threat Detection Service |
| Section 500.07 Access Privileges | • nDiscovery Managed Threat Detection Service |
| Section 500.08 Application Security | • Information Security Policy Development & Assessment |
| Section 500.09 Risk Assessment | • Risk Management Framework Development<br>• Information Security Risk Assessment |
| Section 500.10 Cybersecurity Personnel and Intelligence | • Cybersecurity Partnership Program<br>• nDiscovery Managed Threat Detection Service |
| Section 500.11 Third-Party Service Provider Security Policy | • Service Provider Cybersecurity Assessment Program |
| Section 500.12 Multi-Factor Authentication | • IT Infrastructure Risk Assessment |
| Section 500.13 Limitations of Data Retention | • Information Security Policy Development & Assessment |
| Section 500.14 Training and Monitoring | • nDiscovery Managed Threat Detection<br>• Cybersecurity Awareness Training |
| Section 500.15 Encryption of Nonpublic Information | • IT Infrastructure Risk Assessment |
| Section 500.16 Incident Response Plan | • Incident Response Plan Development<br>• Cyber Incident Response Exercises |
| Section 500.17 Notices to Superintendent | • Incident Response Plan Development |
| Section 500.21 Effective Date | • Executive Cybersecurity Readiness Program |

View all services at www.sagedatasecurity.com/services.