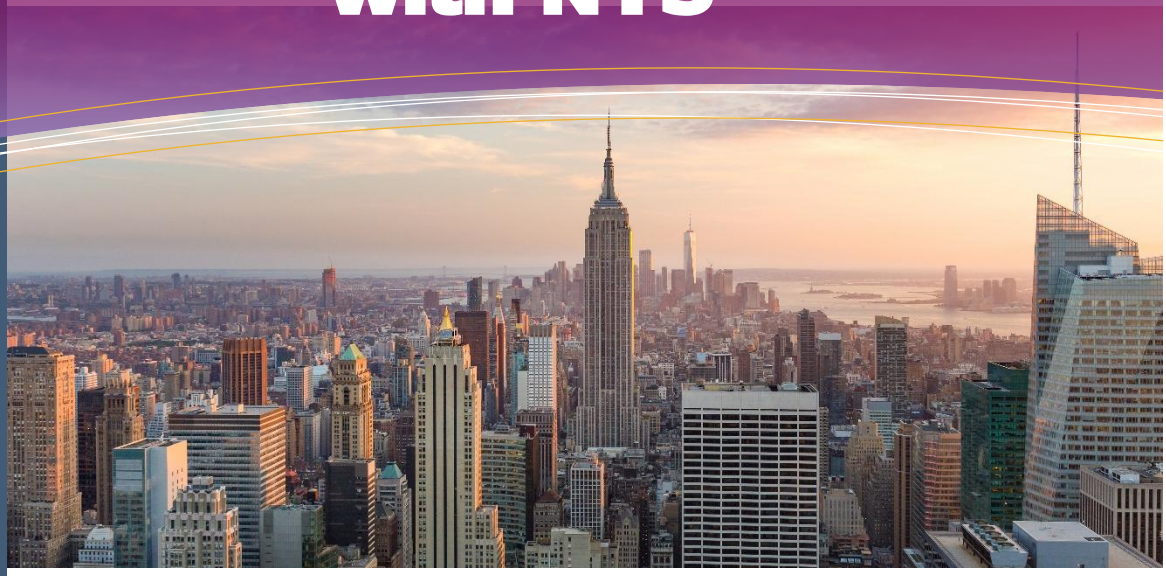
Doing Business with NYS



Summary of 23 NYCRR 500

- Follow cybersecurity best practices
- Assess your risks
- Limit access
- Monitoring and vulnerability checks
- Create an incident response plan
- Designate a CISO

You *can* do it yourself but *should* you?

Placing a call to any client to tell them you were hacked and now the client's data is for sale on the darkweb could ruin a business's reputation. Now, imagine that you had to place that call to the State of New York! Is it worth the risk?

Rochester IT & Business Solutons
www.roc-IT.net

How small businesses can comply with NYDFS Cybersecurity Regulation 23 NYCRR Part 500

New York State will no longer waive regulation 23 NYCRR Part 500 for businesses with fewer than 20 employees and less than $7.5 million in revenue after Nov 1, 2025. The State instituted this regulation two years ago to ensure that the businesses it interacts with don't open the door to cybersecurity threats. While there are still a few exemptions, most now apply across the board.

I know what my fellow SMBs are thinking. It is hard enough to compete with larger companies for these contracts; now there will be another difficult and costly hurdle to overcome! Fortunately, any managed IT Services Provider (MSP) can help you comply. Besides, these requirements are cybersecurity best practices your business should have anyway.

For those that fancy themselves tech savvy, you might even be able to do it yourself.

Understanding the Basics: What NYDFS Requires of You

Think of the regulation as a framework to build a stronger digital fortress around your business and your clients' sensitive information. Here's a simplified look at what's expected:

1. **Your Cybersecurity Plan:** You need a written plan outlining how you'll protect your systems and data. This isn't just about software; it's about policies and procedures.
2. **Knowing Your Risks:** Regularly assess where your weaknesses are. Where is your sensitive data stored? Who has access? What could go wrong?
3. **Multi-Factor Authentication (MFA):** This is like adding a second lock to your digital doors. It means needing something else besides just a password to log in (like a code from your phone).

Tools to Use

There are many solid companies to choose from when shopping for cybersecurity tools. Here are a few to consider. This list is based on our experience and the Gartner Magic Quadrant. We receive no compensation for recommending them.

Multi-factor Authentication-

- Google Authenticator
- Duo
- Microsoft Authenticator

Identity Access Management-

- Microsoft EntraID
- Okta
- OneIdentity

Threat Monitoring-

- Microsoft Defender
- Sentinel One
- Sophos
- Bitdefender

Anti-Virus and VPN

- Avast
- Surfshark
- TotalAV

Some SMB's may be able to comply with 23 NYCRR on their own.

If your company has just a computer or two and uses a few software programs, you may be able to handle it

4 **Limiting Access:** Identity Access Management means only giving employees access to the data and systems they absolutely need for their job. Don't let everyone see everything.

5 **Incident Response Plan:** What happens if you get hacked? You need a clear plan for what to do, who to call, and how to recover.

6 **Vendor Security:** If you use outside companies (like cloud providers or payment processors), you're responsible for ensuring *they* also protect your data.

7 **Data Encryption:** Sensitive information should be scrambled (encrypted) when it's stored or sent, making it unreadable if it falls into the wrong hands

8 **Staff Training:** Your employees are your first line of defense. They need regular training to recognize phishing emails, suspicious links, and other threats.

9. **Vulnerability Checks:** Periodically scan your systems for weaknesses and fix them promptly.

The DIY Approach: Taking the First Steps

For a small business owner, taking a DIY approach often means starting with readily available tools and a lot of personal effort:

- **Policies:** You can find free templates online to draft your cybersecurity policies and incident response plan.
- **MFA:** Implement MFA through services like Google Authenticator or built-in options in Microsoft 365.
- **Access:** Manually review user accounts and permissions.
- **Training:** Use free online cybersecurity awareness videos for your team.
- **Basic Security:** Ensure antivirus software is installed and updated, and firewalls are active.

These are excellent starting points, and for very simple environments, they can provide a foundational layer of protection.

When NOT to do it yourself

If you have more than a computer or two and several employees, the time and cost of managing these requirements yourself grow very quickly. And, it will also outstrip a do-it-yourselfer's skills even faster. Setting up MFA may be no challenge, but how about remediating a cyber threat or setting up Identity Access Management and Role-Based Access Controls? Installing a firewall is not something a layperson should attempt. While taking initial steps yourself is commendable, understanding the depth of NYDFS requirements and the ever-changing cyber threat landscape reveals why many small businesses ultimately partner with Managed Service Providers (MSPs). MSPs have the expertise, the advanced tools, and the dedicated time to not only implement robust solutions access but also to ensure continuous compliance, allowing you to focus on what you do best: growing your business.

The Hidden Hurdles: Why DIY Gets Tricky (and Costly)

Here's where the DIY path often becomes challenging, and where the true value of professional help shines:

1. **Beyond the Basics: Advanced Monitoring and Identity Access:** While basic MFA is essential, truly robust identity and access management involves centralized systems, single sign-on (SSO), and continuous monitoring for unusual login patterns. Most advanced options for centralized security monitoring, sophisticated vulnerability scanning, and identity access management platforms are complex to set up and maintain, often requiring specialized expertise and significant investment in time and technology that's simply not feasible for a non-IT expert.
2. **Time is Money:** Managing cybersecurity isn't a one-time task; it's continuous. Regularly updating policies, conducting deep risk assessments, monitoring logs, and staying abreast of evolving threats takes significant time away from running your actual business.
3. **Keeping Up with Threats:** Cyber threats and regulatory updates evolve constantly. What was secure yesterday might not be today. Without dedicated resources, it's incredibly difficult to stay current and proactive.
4. **The Cost of "Good Enough":** A basic DIY setup might lull you into a false sense of security. If a breach occurs due to an oversight that a more robust, professionally managed system would have caught, the financial penalties, reputational damage, and recovery costs will far outweigh the expense of proactive cybersecurity.
5. **Demonstrating Compliance:** Just *doing* the work isn't enough; you need to *document* it. Proving to the NYDFS that you're compliant requires meticulous record-keeping, audit trails, and reporting, which can be overwhelming to manage manually.

ROC-IT
BUSINESS SOLUTIONS

Contact us for a free consultation.
Info@roc-it.net 585-236-6910
www.roc-it.net

Trend Report

Fractional CTO/CISO

The fractional Chief Information Security Officer (CISO) model is a growing trend, especially among small and medium-sized businesses (SMBs). This is a particularly relevant solution for SMBs subject to the NYDFS regulation, as **one of the NYCRR requirements is to designate a qualified individual as a CISO**. Instead of hiring a full-time, highly-paid executive, businesses can contract a seasoned professional for a fraction of their time. This arrangement provides access to high-level expertise and strategic guidance for a portion of the cost. A fractional CISO can help a company develop and implement a robust cybersecurity program, navigate complex regulations, and ensure that security practices are aligned with business goals. This flexible model allows SMBs to strengthen their security posture and fulfill a crucial regulatory obligation without the financial commitment of a full-time executive salary and benefits..