Cybersecurity Requirements

NYDFS 500 / 23 NYCRR 500
Financial Services

OVERVIEW

On March 1, 2019 the New York State Department of Financial Services Cybersecurity regulations went into full effect. If you operate a **Bank**, **Credit Union**, **Insurance** or **Investment Company**, are a **Mortgage Lender** or **Broker**, or financial service of any kind, your business is required under NYSDFS to comply with the cybersecurity regulations set forth in the 23 NYCRR 500 document.

This can be a little confusing as not all businesses need to comply with every regulation. Regardless of business size, every firm needs to perform a Risk Assessment and write a Cybersecurity Policy. These can take a lot of effort and expertise and it might make sense to bring in a little outside help.

HOW TO COMPLY

Compliance with these regulations cannot be achieved overnight.

The easiest way to get started is a free, DFS 500 Gap Assessment with one of our Micro Solutions cybersecurity experts. In this one-hour meeting, we'll review each requirement of the regulation and your IT setup and provide you with recommendations to close any gaps.

From there, most projects typically follow this process:

- **DFS 500 Gap Analysis/Risk Assessment** – a structured process to compare your business against the DFS 500 Cybersecurity requirements. This identifies gaps that need to be addressed in your policy or IT setup.
- **Information Security Policy** – we'll review or help you draft a policy that addresses your gaps and meets the regulatory requirements.
- **Prioritized Project Plan** – based on your gaps, we'll recommend a plan of action for implementing the technical and cybersecurity changes as required.

As a respected, reputable IT Managed Service Provider, the Micro Solutions team is also available to help you to implement any of the changes required in the Prioritized Project Plan.

CONTACTS

Should you have interest in further details please contact us.

Kristina McCracken – kmccracken@micro-solutions.net – 607-962-1542 x170
Mike Wooldridge – mwooldri@micro-solutions.net – 607-962-1542 x103

REQUIREMENTS

500.01	Definitions	Outline of document definitions
500.02	Cybersecurity Program	Maintain a cybersecurity program to protect the confidentiality, integrity and availability of Information Systems
500.03	Cybersecurity Policy	Written policy or polices outlining the protection of Information Systems and Nonpublic Information stored on those systems
500.04	Chief Information Security Officer	Designated individual to implement and oversee the cybersecurity program and enforce cybersecurity policies
500.05	Penetration Testing and Vulnerability Assessments	Annual Penetration testing and bi-annual Vulnerability assessments required if effective continuous monitoring is not in place
500.06	Audit Trail	Maintain systems designed to reconstruct information to support normal operations; Audit trails to detect and respond to incidents
500.07	Access Privileges	Limit user access to nonpublic information
500.08	Application Security	Secure practices for developing in-house applications; Procedures for evaluating or testing the security of externally developed applications
500.09	Risk Assessment	Periodic assessment of Information Systems based on Cybersecurity Policy
500.10	Cybersecurity Personnel and Intelligence	Qualified personnel, Affiliate, or 3rd party provider to manage risks and oversee performance; Take steps to maintain current knowledge of changing threats and countermeasures
500.11	Third Party Service Provider Security Policy	Written policy outlining minimum cybersecurity practices required to be met by 3rd party providers
500.12	Multi-Factor Authentication	Protect against unauthorized access of nonpublic information
500.13	Limitations on Data Retention	Policy and procedure for secure disposal of nonpublic information
500.14	Training and Monitoring	Monitor and detect unauthorized access of nonpublic information; Provide regular cybersecurity awareness training
500.15	Encryption of Nonpublic Information	Encryption of nonpublic information in transit and at rest
500.16	Incident Response Plan	Written plan designed to respond to, and recover from, and cybersecurity event

Gap Assessment

If you answer yes to any of the following three questions you only need to comply with the regulations highlighted in blue.

1. **Do you have fewer than 10 employees?**
2. **Do you have less than 5 Million in gross annual revenue in each of the last three fiscal years?**
3. **Do you have less than 10 Million is year-end total assets?**

Security Control	Security Requirement	Compliance Status
	Have you filed your annual certificate of compliance with NYS?	
	Have you filed your limited exemption with NYS?	
500.02	Documented Cybersecurity Program	
500.03	Cybersecurity Policy	
500.04	CISO	
500.05	Penetration Testing and Vulnerability Assessments	
500.06	Audit Trail	
500.07	Access Privileges	
500.08	Application Security	
500.09	Risk Assessment	
500.10	Cybersecurity Personnel and Intelligence	
500.11	Third Party Service Provider Security Policy	
500.12	Multi-Factor Authentication	
500.13	Limitations on Data Retention	
500.14	Training and Monitoring	
500.15	Encryption of Nonpublic Information	
500.16	Incident Response Plan	