Sienna Group

New York Department for Financial Services (NYDFS) Cybersecurity Regulations

The New York Department for Financial Services' (NYDFS) Cybersecurity Regulations recently came into force and represent a new code of conduct, impacting all firms operating in the financial services industry within the State of New York. The new regulations, known as 23 NYCRR 500, have a global reach and mandate that companies licensed by or operating in New York State, meet a minimum set of prescribed security requirements.

The 23 NYCRR 500 is designed to protect the data of customers in the financial services sector. Organizations covered by the new cybersecurity regulations include banks and trust companies, insurance companies, mortgage lenders, investment companies, brokers and other financial services providers.

The regulations went into effect on March 1, 2017. The new regulations require that on February 15, 2018 (and annually thereafter), the organization's Board of Directors - or a senior officer, confirm or certify compliance to the DFS, with a "Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations."

Regardless of size or location, it's critical that all companies that operate in the financial services industry within the State of New York, have a cybersecurity program. Section 500.03 mandates that each organization shall implement and maintain a written policy or policies, approved by a Senior Officer or Board of Directors, setting the organization's policies and procedures for the protection of its information systems, and non-public information stored on those information systems. The cybersecurity policy should address the following areas:

- ✓ Information Security
- ✓ Data Governance and Classification
- ✓ Asset Inventory and Device Management
- ✓ Access Controls and Identity Management
- ✓ Business Continuity and Disaster Recovery planning and resources
- ✓ Systems Operations and Availability concerns
- ✓ Systems and Network Security
- ✓ Systems and Network Monitoring
- ✓ Systems and Application Development and Quality Assurance
- ✓ Physical Security and Environmental Controls
- ✓ Customer Data Privacy
- ✓ Vendor and Third-Party Service Provider management
- ✓ Risk Assessment
- ✓ Incident Response

Additionally, Section 500.04 mandates that each organization employ a Chief Information Security Officer (CISO), who will be responsible for overseeing and implementing the organization's cybersecurity program and enforcing its cybersecurity policy.

Sienna Group
9644 Linebaugh Avenue
Tampa, FL 33626

(800) 792-6421
www.siennasecure.com

Other key areas of the regulation include a requirement to:

- Identify cyber risks and conduct penetration testing (minimum annually) and vulnerability assessments (minimum quarterly);
- Secure applications by employing secure development practices for in-house developed applications;
- Implement procedures for assessing & testing security of all third-party developed applications;
- Conduct a periodic risk assessment of the organizations information systems;
- Provide employees with regular cybersecurity awareness training and relevant updates;
- Employ necessary security controls, including encryption to protect non-public data whether in transit or at rest;
- Implement policies and procedures for the secure deletion of any non-public information that is no longer necessary for business operations or for other legitimate business purposes;
- Establish and document an incident response plan

Key Dates/Timelines

Transitional Period

Covered Entities shall have 180 days from the effective date (March 01, 2017) to comply with the requirements set forth except as otherwise specified (below).

One year from effective date:
-500.04 (b) Annual Report
-500.05 Penetration Testing & Vulnerability Assessments
-500.09 Risk Assessment
-500.12 Multi-factor Authentication
-500.14 (b) Cybersecurity Awareness Training

Eighteen months from effective date:
-500.06 Audit Trail
-500.08 Application Security
-500.13 Limitations on Data Retention
-500.14 (a) Activity of Authorized User
-500.15 Encryption of Nonpublic Information

Two years from effective date:
-500.11 Third Party Service Provider Security Policy

The purpose of the regulation is clear and beneficial. It seeks to both define good security practices and ensure that the business owners are responsible for their implementation. In an age where cybersecurity is becoming an ever-greater issue and the threats more prevalent, it's critical that each member of an organization be accountable for the role they play in the security of the information they are creating and sharing.