The NYDFS Cyber Security Requirements Checklist

Cyber Security Program (Section 500.02)

- [ ] Establish a cyber security program based on periodic risk assessments meant to identify and evaluate risks. Effectively protect information systems and nonpublic information; detect, respond to, and recover from cyber events and adhere to all reporting obligations.

Cyber Security Policies (Section 500.03)

- [ ] Create and maintain written policies and procedures to protect your organization's systems and nonpublic information based on the company's risk assessment.

Chief Information Security Officer (Section 500.04)

- [ ] Appoint a CISCO to oversee and implement the required cyber security program. The CISCO may be employed by an affiliate, the regulated entity, or a third party service provider.

  With MDS's Virtual CISCO service, our certified engineers provide your organization with qualified MDS security advisers to assist in guiding security efforts, execute plans and implement a custom strategy for your company. MDS acts as an extension of your team, providing security program assessment, development and management.

Penetration Testing and Vulnerability Management (Section 500.05)

- [ ] MDS Continuous Penetration Testing gives your organization a realistic look at how attackers exploit IT vulnerabilities and actionable ways on how to stop them. Our team not only conducts hundreds of penetration tests annually, but our engineers continuously train on the latest security innovations to ensure we understand this constantly evolving epidemic, learning the latest techniques to identify and negate threats.

Audit Trail (Section 500.06)

- [ ] Securely maintain systems must be designed to: reconstruct fiscal transactions following a security breach and audit trails to detect and respond to cyber security events (maintain records for 3 years).

Application Security (Section 500.08)

- [ ] Security best practices and procedures for internally developed apps is mandatory, along with the periodic evaluating, assessing and security testing of externally developed apps. With MDS financial application security solutions, we can interpret and test today's modern and complex apps, providing your organization with comprehensive and actionable vulnerability reports.

Risk Assessments (Section 500.09)

- [ ] Conduct bi-annual, documented risk assessments that consider threats and the examination of current controls in relation to identifying risk. MDS offers assessments that evaluate the effectiveness of your cyber security controls and provides a prioritized and risk-based security road-map, with detailed recommendations to you can update your security protocol with confidence.

Cybersecurity Personnel and Intelligence (Section 500.10)

- [ ] Qualified cyber security personnel or an "Affiliate or a Third-Party Service Provider" sufficient to manage the organization's risks and to perform or oversee the performance of essential cyber security functions. MDS engineers are highly trained in cyber security to effectively address relevant risks, and continuously attend trainings in order to effectively monitor the evolving threats and corresponding countermeasures.

Multi-Factor Authentication (Section 500.12)

- [ ] To protect unauthorized access to Nonpublic Information, the use of Multi-Factor Authentication (more than one method of credentials to verify user identity) is required for any individual accessing the Covered Entity's internal networks from an external network.

Limitations on Data Retention (Section 500.13)

- [ ] Each Covered Entity is required to have policies and procedures for the secure periodic disposal of specific categories of Nonpublic Information.

Training and Monitoring (Section 500.14)

- [ ] Covered entities are required to implement risk-based policies to monitor the activity of Authorized Users and detect unauthorized access or use of Nonpublic Information. Regular cyber security training for all personnel is also required.

Encryption of Nonpublic Information (500.15)

- [ ] All covered entities must implement encryption controls based on the mandatory risk assessment (Section 500.09), to protect Nonpublic Information held or transmitted over external networks. Such controls must be reviewed and approved by the mandated CISO on an annual basis.

Incident Response Plan (Section 400.16)

- [ ] An established written incident response plan for a responding to and recovering from cyber security events must be implemented. With MDS monitoring your environment, we utilize our preventative and reactive protocol to ensure an immediate response at the first sign of a breach.