NEW YORK STATE OF OPPORTUNITY. | Department of Financial Services

Proposed Cybersecurity Requirements for Financial Services Companies

- **Establishment of a Cybersecurity Program.** Regulated financial institutions will establish a cybersecurity program designed to ensure the confidentiality, integrity and availability of information systems that performs five core cybersecurity functions:
    - Identification of cyber risks.
    - Implementation of policies and procedures to protect unauthorized access/use or other malicious acts.
    - Detection of cybersecurity events.
    - Responsiveness to identified cybersecurity events to mitigate any negative events.
    - Recovery from cybersecurity events and restoration of normal operations and services.

- **Adoption of a Cybersecurity Policy.** Regulated financial institutions must adopt a written cybersecurity policy, setting forth policies and procedures for the protection of their information systems and nonpublic information that addresses, at a minimum, the following:
    - Information security.
    - Data governance and classification.
    - Access controls and identity management.
    - Business continuity and disaster recovery planning and resources.
    - Capacity and performance planning.
    - 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.

- **Chief Information Security Officer**. Regulated financial institutions shall designate a qualified individual to serve as Chief Information Security Officer (CISO) responsible for overseeing and implementing the institution's cybersecurity program and enforcing its cybersecurity policy. The CISO must report to the board, at least bi-annually, to:
  - Assess the confidentiality, integrity and availability of information systems.
  - Detail exceptions to cybersecurity policies and procedures.
  - Identify cyber risks.
  - Assess the effectiveness of the cybersecurity program.
  - Propose steps to remediate any inadequacies identified.
  - Include a summary of all material cybersecurity events that affected the regulated institution during the time period addressed by the report.

- **Third-Party Service Providers**. Regulated entities must have policies and procedures designed to ensure the security of information systems and nonpublic information accessible to, or held by, third-parties and include the following:
  - Identification and risk assessment of third-parties with access to such information systems or such nonpublic information.
  - Minimum cybersecurity practices required to be met by such third-parties.
  - Due diligence processes used to evaluate the adequacy of cybersecurity practices of such third-parties; and
  - Periodic assessment, at least annually, of third-parties and the continued adequacy of their cybersecurity practices.

- **Additional Requirements**. Each cybersecurity program shall include the following:

    - Annual penetration testing and vulnerability assessments.

    - Implementation and maintenance of an audit trail system to reconstruct transactions and log access privileges.

    - Limitations and periodic reviews of access privileges.

    - Written application security procedures, guidelines and standards that are reviewed and updated by the CISO at least annually.

    - Annual risk assessment of the confidentiality, integrity, and availability of information systems; adequacy of controls; and how identified risks will be mitigated or accepted.

    - Employment and training of cybersecurity personnel to stay abreast of changing threats and countermeasures.

    - Multi-factor authentication for individuals accessing internal systems who have privileged access or to support functions including remote access.

    - Timely destruction of nonpublic information that is no longer necessary except where required to be retained by law or regulation.

    - Monitoring of authorized users and cybersecurity awareness training for all personnel.

    - Encryption of all nonpublic information held or transmitted. For in transit data, this requirement is effective one year from the effective date of the regulation. For at rest data, this requirement is effective five years from the effective date as long as there are compensating controls.

    - Written incident response plan to respond to, and recover from, any cybersecurity event.