STATE EMPLOYMENT LAWS




Provided By Touchstone Consulting Group

# Cyber Security Laws - Covered Entity Responsibilities

New York's cyber security laws (CSLs) became effective on **March 1, 2017**. These laws are designed to promote the protection of customer information as well as the information technology systems of affected entities. CSLs require affected companies to assess their specific risk profile and design a program that addresses identified risks.

CSLs in New York were issued for the financial industry to address the increasing number of events that put consumer information and financial information systems at risk. As a result, the New York State Department of Financial Services (DFS) has been given the authority to enforce compliance with these laws. This document provides an overview of the major responsibilities CSLs impose on covered entities.

## RISK ASSESSMENTS

CSLs require **covered entities** to perform risk assessments. These assessments become the basis for developing and maintaining a cyber security program that complies with state law. CSLs define a "covered entity" as any person or institution that operates, or is required to operate, under a license, registration, charter, certificate, permit, accreditation or similar authorization under **banking** law, **insurance** law or **financial services** law.

Risk assessment must be sufficient to inform the covered entity of its vulnerabilities and compliance with CSL requirements. These assessments must be conducted periodically. Risk assessments may be updated as reasonably necessary to address changes to the covered entity's information system (IS), nonpublic information and business operations.

Specifically, the risk assessment must allow for a revision of controls so it can respond to technological developments and evolving threats and consider the particular risks of the covered entity's business operations.

Finally, covered entities must create written policies and procedures, and follow these policies and procedures when conducting risk assessments. Employers are also required to document their risk assessment practices. These policies and procedures include:

- Criteria for the evaluation and categorization of identified cyber security risks or threats facing the covered entity;
- Criteria for the assessment of the confidentiality, integrity, security and availability of the covered entity's IS and nonpublic information, including the adequacy of existing controls in the context of identified risks; and
- Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cyber security program will address the risks.

## MONITORING AND TESTING

CSLs require monitoring and testing as part of a valid cyber security program. To satisfy this requirement, covered entities must implement risk-based policies, procedures and controls that are designed to monitor the activity of authorized users. Policies, procedures and controls should also detect unauthorized access to, use of or tampering with nonpublic information.

Touchstone CONSULTING GROUP
EMPLOYEE BENEFITS • LOCAL AND GLOBAL

# Cyber Security Laws - Covered Entity Responsibilities

Monitoring and testing must be designed in response to a covered entity's risk assessment to evaluate the effectiveness of the entity's cyber security program. In particular, monitoring must include continuous monitoring or periodic penetration testing and vulnerability assessments.

In situations where there is no effective continuous monitoring or where there are no other systems to detect, on an ongoing basis, changes in the IS that may create or indicate vulnerabilities, covered entities must conduct:

- Annual IS penetration testing (this must be determined for each given year based on relevant identified risks and in accordance with the risk assessment); and
- Biannual vulnerability assessments, including any systematic scans or IS reviews that are reasonably designed to identify publicly known cyber security vulnerabilities in the covered entity's IS, based on the risk assessment.

**ENCRYPTION OF NONPUBLIC INFORMATION**

Covered entities must also encrypt nonpublic information, whether this information is being held or transmitted. A covered entity's encryption obligations regarding transmitted information apply to data that is in transit over external networks as well as to data that is at rest.

Covered entities may use effective alternative compensating controls when encrypting nonpublic information in transit over external networks is infeasible. Alternative compensating controls must be reviewed and approved by the entity's **chief information security officer** (CISO) before usage and annually thereafter.

**CYBER SECURITY PERSONNEL**

Each covered entity must also designate a CISO to oversee and implement its cyber security programs, policies and procedures. The CISO may be employed by the covered entity, one of its affiliates or a third-party service provider (additional requirements apply for CISOs employed by third-party service providers). A covered entity's board of directors (or its equivalent) must receive a written report from its CISO at least annually. The report must include an evaluation of the covered entity's cyber security program and material risks. The report must also consider, to the extent applicable:

1. The confidentiality of nonpublic information and the integrity and security of the covered entity's IS;
2. The covered entity's cyber security policies and procedures;
3. The covered entity's material cyber security risks;
4. The covered entity's cyber security program's overall effectiveness; and
5. Any material cyber security events involving the covered entity during the time period addressed by the report.

In addition to the CISO, CSLs require covered entities to:

- Use qualified cyber security personnel. This personnel must be sufficient to manage the covered entity's cyber security risks and perform (or oversee the performance) of the core cyber security functions of the cyber security program;
- Provide sufficient training and updates to cyber security personnel to address relevant risks;
- Provide regular cyber security awareness training for all personnel (must be updated to reflect the risks identified by their risk assessments); and
- Verify that key cyber security personnel take steps to maintain current knowledge of changing cyber security threats and countermeasures.

Covered entities may use an affiliate or third-party service provider to assist in complying with these requirements.

# Cyber Security Laws - Covered Entity Responsibilities

**MULTIFACTOR AUTHENTICATION**

Multifactor authentication, or risk-based authentication, is required for any individual who accesses the covered entity's network from an external network. The authentication must protect against unauthorized access to nonpublic information or the IS.

This requirement may not apply if the covered entity's CISO approves, in writing, the use of reasonably equivalent (or more secure) access controls.

**LIMITATIONS ON DATA RETENTION**

Covered entities must establish policies and procedures that outline how to safely dispose of nonpublic information on a periodic basis. Nonpublic information must be disposed of after it is no longer necessary for business operations or any other legitimate business purpose (including recordkeeping requirements). An exception may be possible when targeted disposal is not reasonably feasible because of how the information is maintained.

**POLICIES AND PROCEDURES**

New York's CSLs also require covered entities to create, implement, and maintain policies and procedures to protect their IS and any nonpublic information contained therein. A covered entity's policies and procedures must be approved by a senior officer or its board of directors (or an equivalent governing body).

The policies and procedures must take into account the entity's risk assessment and address the following areas, to the extent applicable to the covered entity's operations:

- 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 and risk assessment; and
- Incident response.

**EXTERNAL APPLICATIONS AND THIRD-PARTY SERVICE PROVIDER SECURITY POLICY**

In addition, covered entities must also develop and implement policies and procedures to evaluate, assess or test the security of any externally developed applications used by the covered entity within the context of its technology environment.

Similarly, covered entities must implement written policies and procedures to ensure the security of their IS and nonpublic information that are accessible to, or held by, third-party service providers. A covered entity's third-party policies and procedures must also be based on the entity's risk assessment and must address, to the extent applicable:

- The identification and risk assessment of third-party service providers;
- Minimum cyber security practices third-party service providers must satisfy in order for them to do business with the covered entity;
- Due diligence processes used to evaluate the adequacy of third-party service provider cyber security practices, including:
    - Policies and procedures for access controls (including multifactor authentication) to limit access to relevant IS and nonpublic information;

# Cyber Security Laws - Covered Entity Responsibilities

  - Policies and procedures for the use of encryption of nonpublic information (in transit or at rest);
  - Policies and procedures to provide notice to the covered entity in the event of a cyber event that directly impacts the covered entity's IS or the covered entity's nonpublic information held by the third-party service provider; and
  - Representations and warranties addressing the third-party service provider's cyber security policies and procedures that relate to the security of the covered entity's IS or nonpublic information.
- Periodic assessment of third-party service providers based on the risks they present and the continued adequacy of their cyber security practices.

However, a covered entity's agent, employee, representative or designee is not required to develop its own third-party information security policy if he or she follows the covered entity's policy (as long as the covered entity's policy complies with CSL requirements).

**NOTICES**

A covered entity must notify the DFS within **72 hours** from the time it determines that a cyber security event has occurred if:

- The covered entity is required to notify any government body, self-regulatory agency or any other supervisory body of the cyber security event in question; or
- The cyber security event has a reasonable likelihood to cause material harm to any material part to any of the covered entity's normal operations.

**CERTIFICATION AND COMPLIANCE**

Covered entities must submit a report to the DFS every year certifying their compliance with CSLs. Compliance statements must be submitted to the DFS by Feb. 15 of each year, using the form provided in Appendix A. The first certification of compliance report is due on **Feb. 15, 2018**.

All records, schedules and data supporting this certification must be maintained for DFS examination for at least **five years**. Covered entities that identify areas, systems or processes that require material improvement, updating or redesign must also document the identification and the remedial efforts planned. This documentation must also be available for DFS inspection.

**EXEMPTIONS**

New York's CSLs provide general and partial exemptions to a number of entities and individuals. Any individual or entity that ceases to qualify for an exemption, as of its most recent fiscal year end, must comply with all applicable CSL requirements within **180 days** of the fiscal year's end.

***General Exemptions***

A covered entity's employees, agents, representatives and designees who are also covered entities, are exempt from CSLs and are not required to develop their own cyber security programs if they are covered by the cyber security program of the covered entity they work for.

In addition, CSLs provide an exemption for individuals who do not qualify as covered entities under CSLs and are subject to:

- Insurance Law Section 1110;
- Insurance Law Section 5904; or
- Any accredited reinsurer or certified reinsurer that has been accredited or certified under 11 NYCRR 125 (Credit for Reinsurance from Unauthorized Insurers).

# Cyber Security Laws - Covered Entity Responsibilities

***Partial Exemptions***

Partial exemptions apply only to covered entities that meet the requirements specified below. A valid partial exemption applies only to the sections or provisions identified by the exemption. A covered entity that qualifies for any of the exemptions below must file a "Notice of Exemption" using the form provided as Appendix B. The form must be filed within **30 days** of the time the covered entity determines it's exempt.

| Entity Qualification | Exempted Requirements |
|---|---|
| Covered entities that:<br>• Do not directly or indirectly operate, maintain, utilize or control any IS, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess nonpublic information; and<br>• Subject to Article 70 of the Insurance Law, do not, and are not required to, directly or indirectly, control, own, access, generate, receive or possess nonpublic information other than information relating to its corporate parent company (or affiliates). | • Cyber security program<br>• Cyber security policy<br>• Chief information security officer<br>• Penetration testing and vulnerability assessments<br>• Audit trail<br>• Access privileges<br>• Application security<br>• Cyber security personnel and intelligence<br>• Multifactor authentication<br>• Training and monitoring<br>• Encryption of nonpublic information<br>• Incident response plan |
| Covered entities with:<br>• Fewer than 10 workers (employees and independent contractors);<br>• Less than $5 million in gross annual revenue in each of the last three fiscal years from New York business operations (including affiliates); or<br>• Less than $10 million in year-end total assets, calculated in accordance with generally accepted accounting principles (includes affiliate assets). | • Chief information security officer<br>• Penetration testing and vulnerability assessments<br>• Audit trail<br>• Application security<br>• Cyber security personnel and intelligence<br>• Multifactor authentication<br>• Training and monitoring<br>• Encryption of nonpublic information<br>• Incident response plan |