STATE EMPLOYMENT LAWS

Provided By Touchstone Consulting Group

Cyber Security Program Rules

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 entities 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 cyber security program requirements covered entities must satisfy to comply with CSLs in New York.

CYBER SECURITY PROGRAM

New York's CSLs require each **covered entity** to maintain a cyber security program that protects the confidentiality, integrity and availability of its information system (IS). 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.

A covered entity's program is based on that entity's risk assessment, and must be designed to:

1. Identify and assess internal and external cyber security risks that may threaten the security or integrity of nonpublic information stored on the entity's IS;
2. Use defensive infrastructure, policies and procedures to protect the entity's IS (and the nonpublic information stored on it) from unauthorized access, use or other malicious acts;
3. Detect cyber security events;
4. Respond to identified or detected cyber security events to mitigate any negative effects;
5. Recover from cyber security events and restore normal operations and services;
6. Limit user access privileges to an IS that provides access to nonpublic information (must review access privileges periodically); and
7. Comply with all applicable regulatory reporting obligations.

CSLs defines a "**cyber security event**" as any act or attempt, regardless of whether it's successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an IS or the information that is stored within the IS.

Covered entities will be allowed to satisfy their program requirements by adopting the relevant and applicable provisions of a cyber security program maintained by an **affiliate**, but only if those provisions satisfy CSL requirements, as applicable to the covered entity.

An "affiliate" is any person or entity that directly or indirectly controls, is controlled by, is under common control with, or can otherwise direct the management and policies of another person or entity. Affiliate control can be established through, but is not limited to, the ownership of stock.

Touchstone CONSULTING GROUP
EMPLOYEE BENEFITS ▪ LOCAL AND GLOBAL

Cyber Security Program Rules

Cyber security programs must also be designed to reconstruct material financial transactions and include audit trails designed to detect and respond to cyber security events that have a reasonable likelihood of harming any material part of the normal operations of the covered entity.

All documentation and information relevant to the covered entity's cyber security program must be made available to the DFS upon request. Specifically, covered entitles must also maintain records that allow them to reconstruct material transactions for at least **five years** and audit trail records for at least **three years**. Any information subject to CSL requirements that is provided by a covered entity is subject to exemptions from disclosure under banking, insurance, financial services, public officers or any other applicable state or federal law.

NONPUBLIC INFORMATION

Nonpublic information includes all electronic information that is not publicly available. This includes:

- A covered entity’s business-related information, if an unauthorized disclosure, access or use of this information would cause a material adverse impact to the covered entity’s business, operations or security;
- Any information concerning an individual that because of a name, number, personal mark or other identifier can be used to identify the individual, in combination with any one or more of the following data elements:
    - Social Security number;
    - Drivers' license number or other identification card number;
    - Account number, including credit or debit card number;
    - Any security code, access code or password that would permit access to an individual's financial account; or
    - Biometric records.
- Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to:
    - The past, present or future physical, mental, or behavioral health or condition of any individual or a member of the individual's family;
    - The provision of health care to any individual; or
    - Payment for the provision of health care to any individual.

INCIDENT RESPONSE PLAN

Cyber security programs under New York’s CSLs must include a written incident response plan. This plan must be designed to respond promptly to, and help the covered entity recover from, any cyber security incident that has a material effect on the confidentiality, integrity or availability of the covered entity’s IS or the continuing functionality of any aspect of the covered entity’s business or operations.

Specifically, incident plans must address:

- The internal processes for responding to a cyber security event;
- The goals of the incident response plan;
- The definition of clear roles, responsibilities and levels of decision-making authority;
- External and internal communications and information sharing;
- Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
- Documentation and reporting regarding cyber security events and related incident response activities; and
- The evaluation and revision of the incident response plan following a cyber security event (as necessary).

Cyber Security Program Rules

IMPLEMENTATION – TRANSITIONAL PERIOD

Unless otherwise specified, covered entities will have 180 days from the effective date—**Aug. 28, 2017**—to comply with CSL requirements. The table below shows additional transitional periods for specific CSL provisions:

Provision	Compliance	
	Timeline	**Date**
Chief information security officer reports	One year	March 1, 2018
Penetration testing and vulnerability assessments		
Risk assessment		
Multifactor authentication		
Providing regular cyber security awareness		
Audit trail	18 months	Aug. 28, 2018
Application security		
Limitations on data retention		
Implement risk-based policies, procedures and controls		
Encryption of nonpublic information		
Third-party service provider security policy	Two years	March 1, 2019