ComplianceShield™

Solution Map for NYS Department of Financial Services Cyber Law

Easily define, document and deliver a robust cyber security program.

The New York Department of Financial Services (DFS) new law NYCRR 500 Cyber Insurance Requirements for Financial Services Companies ("DFS Cyber Law") sets forth a new regulatory framework that requires all financial institutions doing business in New York to adopt a formal and robust information security program. The following table illustrates how ComplianceShield™ addresses specific requirements of the new law:

NYS DFS Law Requirement	ComplianceShield Solution
Adopt a Cyber Security Program *500.02 (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.*	**CPL Control Library and Wizard** Build a security program in minutes using our Compliance Wizard. Our unique Control Library has over 400 controls addressing the latest technologies, threats and regulatory requirements. Easily map controls to comply with ISO 27002, HIPAA, NIST and PCI-DSS.
Develop and Maintain Written Information Security Policies *500.03 'Cyber Security Policy' - Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors*	**Common Security Policy Library (CPL)** ComplianceShield provides over 40 sample information security policies that address each of the required areas of the DFS Law. Including: (b) data governance and classification; (c) asset and device management; (d) identity and access controls; (e) business continuity and DRP; (f) IT operations; (g) systems and network security; (h) Monitoring; (i) application development; (j) physical and environmental security; (k) customer data privacy; (l) Third Party Service Providers; (m) risk assessment; and (n) incident response.
Assign Management Accountability *Section 500.10 Cybersecurity Personnel and Intelligence. (1) utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.02(b)(1)-(6);*	**Define and Assign Information Security Roles** ComplianceShield contains a library of built-in security and privacy job descriptions, saving hundreds of hours of development. Easily assign security program elements to individuals based on defined security roles, including those of third parties.

Assign Chief Information Security Officer

500.04 - Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, "Chief Information Security Officer" or "CISO").

Virtual CSO Services

ComplianceShield customers have access to qualified information security professionals on a fractional basis. Clients can easily outsource part or all of their cyber security program to expert staff with many years of practical experience.

Educate and Train Users

500.14 Training and Monitoring.
(b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

Security Awarness Training Library

Use our built-in security awareness training module to educate employees and contractors on basic security awareness principles. Our training covers key topics including: Access Control, Email and Web Usage, phishing, Mobile Security, Information Classification and security incident reporting.

Manage Third Party Vendor Risk

500.11 (a) Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers

Vendor Risk Management

ComplianceShield enables automation of third party risk management. Cyber Risk Scoring allows clients to quickly assess the security and privacy risk of vendors. Security control reporting and secure evidence exchange can eliminate spreadsheets and other manual methods. Third party security policies and controls help define the entire process.

Track and Manage Compliance Evidence

Section 500.02 (d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

Compliance Reporting and Management

Manage and track progress at every step by assigning controls based on the role of each user. Easily track the implementation of each critical information security control using our Cyber Maturity Scoring. Manage and store evidence of control status for easy internal or external audit.

Support Management Attestation

Section 500.17 (b) Annually each Covered Entity shall submit to the superintendent a written statement covering the prior calendar year. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years.

Compliance Reporting and Metrics

Quickly demonstrate cyber security due-diligence to senior management, auditors, customers and insurers with a few simple reports. Risk Scoring Reports provide a simple overview of your entire information security program.

About Information Shield

Information Shield is a global provider of security policy and IT security compliance solutions that enable organizations to simplify compliance with international security and privacy regulations. Information Shield products are used by over 9000 customers in 60 countries worldwide.

InformationShield

Information Shield, Inc.
www.informationshield.com
sales@informationshield.com
P: 888.641.0505
F: 866.304.6704