NY SHIELD Act
Security Program Requirements

(for persons and businesses that are not considered Small Businesses or covered by other laws)

February 17, 2020

info@assuredSPC.com

Assured SPC

Security Program safeguard requirements

Administrative Safeguards	NY SHIELD Act language
Security leadership	(1) designates one or more employees to coordinate the security program;
Risk Management	(2) identifies reasonably foreseeable internal and external risks; (3) assesses the sufficiency of safeguards in place to control the identified risks;
Employee training	(4) trains and manages employees in the security program practices and procedures;
Service Provider management	(5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
Program Management	(6) adjusts the security program in light of business changes or new circumstances; and
Technical Safeguards	
Risk Management	(1) assesses risks in network and software design;
DPIA	(2) assesses risks in information processing, transmission and storage;
SIEM	(3) detects, prevents and responds to attacks or system failures; and
Testing of controls (procedures, vulnerability testing, penetration testing)	(4) regularly tests and monitors the effectiveness of key controls, systems and procedures; and
Physical Safeguards	
Risk Management	(1) assesses risks of information storage and disposal;
Physical access management	(2) detects, prevents and responds to intrusions;
Data access management	(3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
Physical data disposal	(4) disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

About Assured SPC

Assured SPC has expertise in the lifecycle of information security and privacy programs. We assist organizations with requirements for compliance including HIPAA, NIST and CCPA to implement reasonable security procedures and practices and to implement the requirements and objectives of security objectives and privacy laws.

We regularly help organizations prepare for AICPA SOC2 audits and HITRUST CSF assessments. We also offer virtual c-level leadership for SMB businesses, including Chief Information Officer (vCIO), Chief Information Security Officers (vCISO) and Chief Privacy Officer (vCPO) services.