New York State Department of Financial Services

Cybersecurity Requirements for Financial Services Companies

Requirements to be Completed by August 28, 2017

Section	Title	Description
500.03	Cybersecurity Policy	Create and maintain a policy or policies, approved by a Senior Officer, Board of Directors, or equivalent governing body, for the protection of its Information Systems and Nonpublic Information stored on internal and external Information Systems.
500.04(a)	Assign Chief Information Security Officer (CISO)	Designate a qualified individual responsible for overseeing and implementing the Cybersecurity Program and enforcing the Cybersecurity Policy. This person may be employed by the Institution, one of its Affiliates, or a Third-Party Service Provider.
500.07	Access Privileges	Limit user access privileges to Information Systems that provide access to Nonpublic Information with periodic reviews.
500.10	Cybersecurity Personnel & Intelligence	In addition to the appointment of a CISO, all entities must utilize qualified Cybersecurity personnel to manage cybersecurity risks and core functions. This person(s) can be employed by the Institution, an Affiliate, or a Third-Party Service Provider.
500.16	Incident Response Plan	Create a response plan designed to promptly respond to – and recover from – any Cybersecurity event that affects the confidentiality, integrity, or availability of the covered institution's Information Systems or the continuing functionality of any aspect of business or operations.
500.17	Notices to Superintendent	Prompt notification of any Cybersecurity event within 72 hours to the Superintendent where notice is required to be provided to any supervisory body and/or potential harm to any material part of normal operations.