New York State Department of Financial Services

Cybersecurity Requirements for Financial Services Companies

Requirements to be Completed for March 1, 2018

Section	Title	Description
500.04(b)	CISO Begins Reporting to Board of Directors	The Chief Information Security Officer is required to report, in writing, to the Board of Directors, or equivalent governing body, at least once a year. This report includes the status and effectiveness of the Cybersecurity Program as well as any material Cybersecurity Risks.
500.05	Begin Annual Penetration Testing and Vulnerability Assessments	In accordance with your Cybersecurity Risk Assessment, institutions must perform continuous monitoring, annual penetration tests and bi-annual vulnerability assessments to assess the effectiveness of your Cybersecurity Program.
500.09	Commencement of Periodic Risk Assessments	Periodic Risk Assessments should be conducted to continually address changes to your Information Systems, business operations and nonpublic information. This activity should be carried out in accordance with your written Risk Assessment policies and procedures.
500.12	Implement Multi-Factor Authentication	Each institution is required to use effective Cybersecurity Controls, which may include Multi-Factor Authentication or Risk-Based Authentication. This helps protect against unauthorized access to Nonpublic Information and Information Systems. This is required for any individual accessing the Institution's internal network from an external network.
500.14(b)	Provide Regular Cybersecurity Awareness and Training for All Personnel	Provide regular Cybersecurity Awareness Training for all personnel that is updated to reflect risks identified by the Risk Assessment.