New York State Department of Financial Services

Cybersecurity Requirements for Financial Services Companies

Requirements to be Completed by September 3, 2018

Section	Title	Description
500.06	Develop and Maintain Audit Trail of Transactions	All institutions reporting the NY DFS are required to have a mechanism to reconstruct material financial transactions to support normal operations. Audit Trails must be in place to detect and respond to Cybersecurity events that may materially harm any part of your normal operations.
500.08	Implement Procedures, Guidelines and Standards for In-House and Externally Developed Applications	Ensure the use of secure development practices for in-house developed applications, as well as procedures for evaluating, assessing and testing the security for externally-developed applications.
500.13	Implement Policies and Procedures for Disposal of Nonpublic Data	Policies and procedures should be in place for the periodic, secure disposal of any nonpublic information identified in Section 500.01 deemed to be unnecessary for business operations or business purposes.
500.14(a)	Implement Policies, Procedures and Controls for User Monitoring	These risk-based policies, procedures and controls are designed to monitor the activity of authorized and unauthorized users accessing or tampering with nonpublic information.
500.15	Implement Encryption of Nonpublic Information	Each institution is required to implement controls, including encryption, to protect all nonpublic information both in transit over external networks and at rest.