THE NYDFS CYBER SECURITY REQUIREMENTS CHECKLIST

KYBER SECURITY

The following checklist summarizes NYDFS Security Rule requirements that should be implemented by covered entities and business associates. For additional resources concerning Security Rule requirements and compliance assistance, see the Office of Civil Rights (OCR) website.

The Security Rule is subject to periodic amendment. Users should review the current rule requirements on a regular basis to ensure continued compliance.

NYDFS Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status (Complete, N/A)
Administrative Safeguards		
Cyber Security Program (Section 500.02)	Establish a cybersecurity program through periodic internal and external risk assessments that may threaten the security or integrity of Nonpublic Information on Information Systems. The program must include processes for detection, response, recovery and reporting obligations.	
Cyber Security Policies (Section 500.03)	Based on your risk assessment written policies and procedures must be created and maintained to protect Nonpublic Information on your Information Systems.	
Chief Information Security Officer (Section 500.04)	Designate a qualified Chief Information Security Officer. The CISO may be employed internally or by a Third Party Service Provider.	
Penetration Testing and Vulnerability Management (Section 500.05)	Annual Penetration Testing and bi-annual vulnerability assessments of Information Systems based on relevant identified risks in accordance with your Risk Assessment.	
Audit Trail (Section 500.06)	Audit trails are required not fewer than 5 years to reconstruct material financial transtions and not fewer than 3 years for Cybersecurity Events that materially harm normal operations of your business.	
Access Privileges (Section 500.07)	User access privileges to Information Systems of Nonpublic Information must be limited where applicable and reviewed periodically.	
Application Security (Section 500.08)	To ensure the security of applications, whether internally or externally developed, they must have procedures, guidelines and standardsimplemented for evaluation and assessment.	

338 Commerce Drive, Fairfield, CT 06825 | 50 Inwood Road, Rocky Hill, CT 06067 | 1570 Westminster Street, Providence, RI 02909
P: 203.333.4444 sales@kybersecure.com

THE NYDFS CYBER SECURITY REQUIREMENTS CHECKLIST

KYBER SECURITY

NYDFS Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status (Complete, N/A)
Administrative Safeguards		
Risk Assessments (Section 500.09)	Periodic risk assessments that address changes of Information Systems, Nonpublic Information or business operations are required to inform the design and changes of the cybersecurity program.	
Cybersecurity Personnel and Intelligence (Section 500.10)	Cybersecurity personnel, whether internal or Third Party Service Provider, must sufficiently manage cybersecurity risks and oversee the performance of core cybersecurity functions.	
Third Party Service Provider (Section 500.11)	Written policies and procedures must be implemented to ensure the security of Information Systems and Nonpublic Information that are accessible or held by Third Party Service Providers.	
Multi-Factor Authentication (Section 500.12)	Multi-Factor Authentication (utilizing more than one method of login credentials to verify user authentication) is required to protect against unauthorized access to Nonpublic Information or Information Systems.	
Limitations on Data Retention (Section 500.13)	On a periodic basis the secure disposal of any Nonpublic Information that is no longer necessary for legitimate business operations is required unless it must be retained by law or regulation.	
Training and Monitoring (Section 500.14)	Authorized Users activity must be monitored in order to detect unauthorized access or tampering with of Nonpublic Information. Cybersecurity awareness training is required for all personnel.	
Encryption of Nonpublic Information (Section 500.15)	Controls must be implemented to protect Nonpublic Information that is held or transmitted over external networks and at rest via encryption. The CISO must annually review and approve these controls.	
Incident Response Plan (Section 500.16)	A written incident response plan must be designed to respond and recover from any Cybersecurity Event materially affecting the confidentiality, integrity or availability of Information Systems.	

338 Commerce Drive, Fairfield, CT 06825 | 50 Inwood Road, Rocky Hill, CT 06067 | 1570 Westminster Street, Providence, RI 02909
P: 203.333.4444 sales@kybersecure.com