Kiteworks

COMPLIANCE BRIEF

NYDFS Cybersecurity Compliance Support With Kiteworks

Meeting New York State Financial Services Requirements Through Secure Content Communications

The New York State Department of Financial Services (NYDFS) Second Amendment to 23 NYCRR 500 establishes comprehensive cybersecurity requirements designed to protect nonpublic information and information systems of financial services companies. This regulation applies to all covered entities operating under licenses, registrations, charters, or similar authorizations under New York's Banking Law, Insurance Law, or Financial Services Law, regardless of their physical location or additional regulatory oversight. Financial institutions, insurance companies, and other financial services firms must implement robust cybersecurity programs encompassing vulnerability management, access controls, encryption, incident response planning, and third-party risk management. The regulation became effective November 1, 2023, with transitional compliance periods ranging from 30 days to two years depending on specific requirements, requiring full implementation of asset management and multi-factor authentication by November 1, 2025. Noncompliance carries significant penalties including potential regulatory sanctions, mandatory remediation timelines, and reputational damage that could disrupt business operations and customer trust. Kiteworks provides a comprehensive secure content communications platform that supports NYDFS-regulated entities that need to achieve and maintain compliance through encrypted file sharing, secure collaboration tools, and detailed audit capabilities that address the regulation's stringent data protection and reporting requirements. Here's how:

Cybersecurity Framework With Zero-Trust Architecture and Comprehensive Security Functions

Section 500.2 establishes the foundational framework requiring covered entities to maintain comprehensive cybersecurity programs that protect confidentiality, integrity, and availability of information systems and nonpublic data. The regulation mandates programs designed to perform six core functions: identifying risks, protecting systems, detecting events, responding to incidents, recovering operations, and fulfilling reporting obligations. Kiteworks addresses these requirements through its hardened virtual appliance deployment that minimizes attack surfaces using zero-trust assume-breach architecture with tiered component positioning that partitions service layers to block lateral movement and exfiltration.

Solution Highlights

- **Zero-trust architecture**
- **SIEM integration**
- **Role-based and attribute-based access controls**
- **Strong double encryption**
- **Embedded web application firewall**
- **Multi-factor authentication**

The platform provides comprehensive cybersecurity functions across all required areas through asset management capabilities that classify data within attribute-based access control policies, native user management with integration to external identity systems like LDAP and Microsoft Active Directory, and consolidated normalized logging across all communication channels with continuous SIEM feeds via syslog and Splunk Forwarder. Response capabilities include automated notifications, automatic file quarantines, comprehensive forensic data, and rapid vulnerability patch delivery with one-step updates, while recovery functions encompass replicated data and failover systems.

Access Privileges and Management Supported With Role-Based Controls and Automated User Life-Cycle Management

Section 500.7 establishes strict controls over user access to information systems containing nonpublic information, requiring least-privilege principles, limited privileged accounts, annual access reviews, secured remote protocols, and prompt access termination upon employee departures. Class A companies must deploy privileged access management solutions and automated common password blocking to create comprehensive access governance frameworks. Kiteworks implements comprehensive access privilege management through role-based access controls that assign permission sets to users controlling feature and resource access, combined with attribute-based access controls governing data access dynamically based on data attributes, user attributes, and attempted actions. The system uses least-privileged defaults where users automatically receive minimal necessary privileges, requiring administrators to explicitly enable elevated permissions with separation of duties through eight default admin roles meeting most regulatory requirements and custom roles for specific customer needs. Integration with LDAP and Microsoft Active Directory sources enables automatic user onboarding, offboarding, and role updates with flexible profile assignments based on LDAP attributes. The platform provides privileged access monitoring through automated detection of potentially risky settings when administrator users make changes away from safe defaults, typically requiring authorization sign-off before settings can be saved, while credential-based authentication prevents auto-filling and storage of credentials across browsers.

Monitoring and Training Enabled by Real-Time Logging and Embedded Security Controls

Section 500.14 combines continuous security monitoring capabilities with mandatory cybersecurity awareness training requirements, mandating risk-based controls for monitoring authorized user activities, detecting unauthorized access, protecting against malicious code through web and email filtering, and providing annual social engineering training. Class A companies must implement endpoint detection solutions and centralized logging systems to create comprehensive security operations and human awareness defense layers. Kiteworks maintains comprehensive log data for security and compliance activities, automatically cleaning, normalizing, standardizing, and aggregating information into unified streams unlike many competitor solutions. The platform includes an embedded web application firewall that detects and blocks web and REST API attacks with zero maintenance requirements because Kiteworks engineers tuned rulesets specifically for secure content communication use cases. Comprehensive consolidated normalized logging spans all communication channels and system components with continuous SIEM feeds via syslog and Splunk Forwarder, while all customers must run embedded antivirus or integration enforcement as a renewal condition. The system feeds SIEMs in real time, unlike competitors that delay log entries up to 72 hours, and maintains evolving libraries of patterns detecting suspicious network activities and virtual appliance intrusions using artificial intelligence and other technologies for comprehensive intrusion and anomaly detection capabilities.

Kiteworks delivers comprehensive cybersecurity capabilities that directly address NYDFS Second Amendment requirements across critical compliance domains. The platform's zero-trust architecture with hardened virtual appliance deployment creates robust protection layers while comprehensive logging and SIEM integration ensure continuous monitoring and incident detection. Role-based and attribute-based access controls implement least-privilege principles with automated user life-cycle management, while comprehensive encryption protects data at rest and in transit using industry standards.

The embedded web application firewall and automated vulnerability management capabilities provide proactive threat protection, while business continuity features including replicated data and failover systems ensure operational resilience. Through consolidated normalized logging, real-time SIEM feeds, and comprehensive audit logs, Kiteworks enables NYDFS-regulated entities to maintain detailed documentation required for regulatory compliance while supporting the six core cybersecurity functions mandated by the regulation. This integrated approach allows financial services companies to efficiently achieve compliance requirements while maintaining secure, auditable operations across all communication channels and data workflows.