COMPLIANCE GUIDE

How Zero Networks Helps with NYDFS Regulation Requirements



The New York Department of Financial Services (NYDFS) cybersecurity requirements, also known as 23 NYCRR Part 500, mandates that financial institutions implement robust cybersecurity measures to protect sensitive customer information and the integrity of their IT systems.

Below are the specific requirements where Zero Networks helps achieve NYDFS compliance.

Requirement	Description	How Zero Helps
Section 500.02	**Cybersecurity Program:** Each covered entity must maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of its information systems, based on a risk assessment, and capable of identifying, protecting against, detecting, responding to, and recovering from cybersecurity events.	Zero's Network Segmentation satisfies Cybersecurity Program requirements by dividing networks into smaller, isolated segments, enhancing the protection of information systems and ensuring that only authorized users can access sensitive data. This aligns with the regulation's goal of safeguarding the confidentiality, integrity, and availability of information systems. It also blocks ransomware and lateral movement.
Section 500.03	**Cybersecurity Policy:** Each covered entity is required to implement and maintain a written cybersecurity policy, approved by a senior officer or the board of directors, which addresses specific areas of cybersecurity based on the entity's risk assessment.	Zero Networks enables organizations to implement automated microsegmentation and multi-factor authentication (MFA), which align with the regulation's mandate to address specific areas of cybersecurity and implement a resilient network architecture, mitigating cyber risk.
Section 500.07	**Access Privileges:** Each covered entity is required to limit user access privileges to information systems that contain nonpublic information, based on the entity's risk assessment,and to periodically review these access privileges.	Zero's Network Segmentation restricts user access privileges to only what is necessary for operational needs, preventing unauthorized access and lateral movement within the network. This approach is enhanced by multi-factor authentication (MFA), which adds an extra layer of security for privileged access, ensuring compliance with the regulation's mandate to periodically review and limit user access privileges.

Requirement	Description	How Zero Helps
Section 500.09	**Risk Assessment:** Each covered entity must conduct periodic risk assessments to inform the design of their cybersecurity program, ensuring it addresses identified risks and is updated as necessary to reflect changes in technology and emerging threats.	Zero effectively mitigates the impact of potential breaches by blocking lateral movement and the spread of ransomware. By automatically microsegmenting networks and closing all sensitive ports, organizations can dynamically enforce security policies based on real-time network behavior. This, layered with just-in-time MFA, aligns with the regulation's requirements of conducting periodic risk assessments to address identified risks and emerging threats.
Section 500.11	**Third-Party Service Provider Security Policy:** Requires covered entities to develop and implement risk-based policies and procedures to ensure the security of information systems and nonpublic information accessible to or held by third-party service providers.	Zero enables organizations to automatically create and enforce security policies that control and monitor third-party access to specific systems using microsegmentation and multi-factor authentication. This approach restricts third-party access to essential resources, ensuring compliance with regulations for secure handling of information systems, sensitive data, and nonpublic information.
Section 500.12	**Multi-Factor Authentication (MFA):** Covered entities are required to implement multi-factor authentication (MFA) for any individual accessing their internal networks from an external network, unless the Chief Information Security Officer (CISO) approves the use of reasonably equivalent or more secure access controls.	Zero's network-layer MFA protects and verifies all access to internal systems from external networks, including privileged user access. This meets the regulations MFA mandate but also enhances it; by applying MFA at the port level, Zero provides comprehensive protection for sensitive assets and prevents unauthorized access even if credentials are compromised. It also allows organizations to apply MFA to anything - legacy applications, databases, OT and IoT devices, and more.
Section 500.14	**Training and Monitoring:** Covered entities must implement policies and procedures for monitoring authorized users and detecting unauthorized access, use, or tampering with nonpublic information, with additional requirements for Class A companies to implement endpoint detection and response solutions and centralized logging.	Zero's identity-based microsegmentation, combined with just-in-time multi-factor authentication (MFA), enables organizations to effectively control and monitor access to network assets. This setup allows for detailed tracking of user activities, prevents unauthorized lateral movement, and provides Class A companies with endpoint detection and response capabilities for enhanced security.

ZERO. Networks

Connect with the Zero team to discover how you can streamline your NYDFS compliance with automated microsegmentation that deploys in just 30 days.

Book a Demo