WHITE PAPER

Aligning With NYDFS Requirements

Foreword

The New York Department of Financial Services (NYDFS) Cybersecurity Regulation, also known as Part 500, was established to strengthen the cyber resilience of financial institutions and other regulated entities in the face of growing cybersecurity threats. NYDFS mandates comprehensive security measures, including risk assessments, incident reporting, access controls, and data protection, to safeguard sensitive nonpublic information (NPI) and ensure the integrity of financial systems. Aligning with NYDFS requirements is crucial for organizations not only to avoid substantial penalties for non-compliance but also to protect their customers, data, and reputation from increasingly sophisticated cyberattacks. Compliance with Part 500 enhances an organization's overall cybersecurity posture, reduces the risk of costly breaches, and fosters trust with clients and regulators in an industry that demands stringent security controls.

Armis has been instrumental in helping organizations align with NYDFS Cybersecurity Regulation (Part 500) and other critical financial industry requirements by providing real-time visibility, security, and control over all connected devices—both managed and unmanaged—across an organization's network. As financial institutions face increasingly stringent regulations, Armis Centrix™ offers continuous monitoring and automated risk assessments that ensure compliance with key mandates, such as incident detection, user access management, and asset inventory tracking. By identifying vulnerabilities, detecting anomalies, and providing detailed reporting, Armis enables organizations to maintain a strong security posture, satisfy regulatory requirements like multifactor authentication (MFA), and streamline the process of filing compliance certifications. In addition to NYDFS, Armis helps organizations meet other financial regulations such as PCI-DSS and SOX, protecting sensitive data and enhancing operational resilience in a dynamic operating environment.

01 File Annual Cybersecurity Compliance Forms (§ 500.17(b))

Armis helps organizations maintain ongoing visibility and security posture, which supports the documentation needed for certification of compliance or acknowledgement of noncompliance. Through continuous monitoring, automated reporting, and data collection, Armis provides evidence of security activities, enabling Covered Entities to assess their adherence to Part 500 requirements for the prior year. This helps reduce the burden of gathering necessary information for the annual certification or noncompliance acknowledgment.

02 Review and Approve Written Cybersecurity Policies (§ 500.3)

Armis delivers comprehensive insight into an organization's devices, systems, and networks, which ensures that written cybersecurity policies remain aligned with the actual security landscape. The platform's real-time visibility and analytics enable decision-makers to review and refine policies based on the current threat environment and network infrastructure, contributing to compliance with annual review and approval requirements.

03 Review and Update Risk Assessment (§ 500.9(a))

Armis continuously monitors an organization's assets and networks, providing a real-time risk assessment based on device behavior and vulnerabilities. The platform's ability to track and assess both managed and unmanaged devices allows organizations to easily update their cybersecurity risk assessments, especially after significant changes in technology or business operations. Armis's insight into changes in hardware, software, and network configurations allows risk assessments to be more accurate and timely.

04 Cybersecurity Awareness Training (§ 500.14(a)(3))

Armis supports the implementation of training by identifying and reporting on cybersecurity incidents such as device misuse. By providing visibility into real-world attack vectors and vulnerabilities, organizations can tailor their cybersecurity awareness training to current risks, which ensures more effective employee education.

05 Review and Manage User Access Privileges (§ 500.7(a)(4))

Armis assists in managing and auditing user access privileges by monitoring all connected devices and users accessing the information system. It can help identify excessive privileges, unauthorized access, and access anomalies, enabling companies to review, limit, and revoke unnecessary access. As access reviews become mandatory by May 2025, Armis's ability to track user activities in real-time will become an invaluable tool for compliance.

06 Third-Party Service Provider Assessments (§ 500.11(a)(4))

Armis provides visibility into third-party devices and systems connected to the network, allowing organizations to assess the cybersecurity practices of their service providers. The platform helps Covered Entities assess risk and monitor the security posture of third-party vendors, enabling ongoing compliance with the requirement to ensure that third-party providers have adequate cybersecurity protections.

07 Report Cybersecurity Incidents and Extortion Payments (§ 500.17(a), 500.17(c))

Armis detects and alerts on anomalies, vulnerabilities, and breaches in real time. Its ability to identify unusual device behaviors allows for rapid detection of cybersecurity incidents, which supports timely reporting to the NYDFS. In the event of ransomware or extortion attempts, Armis can provide critical data to support required reporting, such as incident details and device activity logs.

08 Secure Disposal of Nonpublic Information (NPI) (§ 500.13(b))

Armis assists with tracking and managing all devices and data flows within the organization, ensuring that NPI is securely disposed of when it is no longer needed. By identifying devices that store or access sensitive information, organizations can better enforce data retention policies and manage the proper disposal of data.

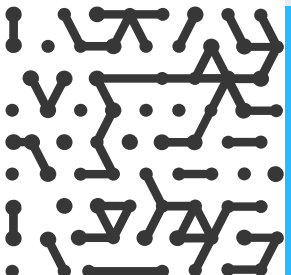
09 Implement Multifactor Authentication (MFA) (§ 500.12)

Armis enhances security monitoring by verifying that MFA is in place for remote access and privileged accounts. By detecting devices attempting to access the network without proper MFA credentials or compensating controls, Armis helps organizations maintain compliance with this critical security measure.

10 Develop and Maintain Up-to-Date Asset Inventory (§ 500.13(a)(2))

Armis automatically generates a comprehensive, real-time inventory of all managed and unmanaged assets connected to an organization's network, ensuring continuous compliance with the asset inventory requirement. This capability will be particularly important when the November 1, 2025, deadline for asset inventory maintenance becomes effective.

By providing visibility, control, and continuous monitoring across all connected devices and assets, Armis acts as a comprehensive tool to help organizations meet the stringent cybersecurity requirements outlined by NYDFS Part 500.



Solution Summary

Asset Visibility

Armis provides comprehensive visibility into all connected devices within an organization's network, including unmanaged and IoT devices. This capability aligns with NYDFS's regulations, which emphasize the need for financial institutions to have detailed knowledge of all their assets and potential vulnerabilities.

Risk Assessment

Armis helps organizations assess risks associated with their connected devices. This includes identifying vulnerabilities (and other security findings), tracking device behaviors, and assessing the potential impact of security incidents. Such capabilities support NYDFS's requirement for regular risk assessments and the implementation of appropriate safeguards.

Threat Detection and Response

Armis offers real-time monitoring and threat detection for connected devices along with risk prioritization, helping organizations respond to potential security incidents swiftly. This aligns with NYDFS regulations that mandate prompt detection and response to cybersecurity threats.

Compliance Reporting

Armis's solutions can assist organizations in maintaining records and generating reports related to their cybersecurity posture, which is crucial for compliance with NYDFS's reporting requirements.

Security Controls

Armis Centrix™ helps enforce security policies and compensating controls across all connected devices, supporting NYDFS's requirements for implementing robust cybersecurity measures.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial