The AWN CyberSOC™ Service Simplifies Compliance for NY DFS Cybersecurity Requirements (23 NYCRR 500)

AWN CyberSOC™ Service

- Superior managed threat detection and response
- Dedicated security expertise for your IT team
- 24/7 monitoring with unlimited log sources

Benefits

- Simplifies 23 NYCRR 500 compliance with customized reporting
- Monitors access to information systems and non-public information on-premises and in the cloud
- Provides real-time alerts on unauthorized access

The New York State Department of Financial Services (DFS) announced 23 NYCRR 500 has become effective 1 March 2018 after a period of comments.[1] Also known by the name "Cybersecurity Requirements for Financial Services Companies," the New York state regulations address concerns that financial firms face an escalating volume and sophistication of cyberthreats.

23 NYCRR 500 intends to establish minimum regulatory standards to promote the protection of customer information as well as the information technology systems of regulated entities. To meet these new regulations, each financial firm must first assess its risk profile and then design a program that addresses its risks. Doing so takes a good deal of time and planning. The requirements are broad, and range from general guidance to specifics such as maintaining an audit trail.

Many financial services organizations will find meeting these new regulations a significant challenge. However, there's no need to go it alone. Arctic Wolf helps you meet many of the 23 NYCRR 500 requirements with a turnkey SOC-as-a-service solution—the AWN CyberSOC.

Who Is Affected

The NY DFS 23 NYCRR 500 affects any entity covered under the New York State Banking Law, the New York State Insurance Law or the New York State Financial Services Law. This includes state-chartered banks, licensed lenders, trust companies, mortgage companies, foreign banks licensed to operate in New York, and insurance companies doing business in New York.

[1] Formally known as Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York. https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

How the AWN CyberSOC™ Service Helps Meet Requirements of New York 23 NYCRR 500

The columns below map the requirements in 23 NYCRR 500 to the functionality provided by the AWN CyberSOC.

23 NYCRR 500 Requirement	Arctic Wolf SOC-as-a-Service Capability
Section 500.02 Cybersecurity Program Maintain a cybersecurity program based on a risk assessment that identifies internal and external cybersecurity risks, implement policies and procedures that detect cybersecurity events, and responds and recovers.	Arctic Wolf continuously monitors on-premise and cloud resources and displays in a customer portal a rating of the financial institution's security posture, including vulnerability management status, and outstanding security incidents.
Section 500.05 Penetration Testing and Vulnerability Assessments Maintain a program to continuously monitor and assess the environment, periodically perform penetration testing and vulnerability assessments. This includes annual penetration testing and bi-annual vulnerability assessments.	Arctic Wolf delivers monthly vulnerability assessment reports and the AWN CyberSOC provides a rating of their overall security posture.
Section 500.06 Audit Trail Securely maintain systems, including audit trails to detect and respond to cybersecurity events. Maintain cybersecurity event records for three years (five years for material financial transactions).	The AWN CyberSOC can maintain audit trail records for three or more years (default is 90 days).
Section 500.07 Access Privileges Limit user access privileges to information systems, periodically review access privileges.	Arctic Wolf audits changes to Active Directory (AD), group policies, Exchange and file servers, and flags unauthorized actions, which enables development/ enhancement of the required policies and procedures. Arctic Wolf monitors failed/successful logins/ logoffs and all password changes to prevent excessive help desk calls.
Section 500.09 Risk Assessment Conduct a periodic risk assessment of information systems.	The Arctic Wolf Concierge Security™ team manages periodical scanning of externally-exposed systems for vulnerabilities and continually monitors network traffic and log files for potential compromise.
Section 500.10 Cybersecurity Personnel and Intelligence Utilize qualified cybersecurity personnel or a qualified "affiliate or a third-party service provider" to manage the organization's risks and perform or oversee the performance of the core cybersecurity functions.	The AWN CyberSOC is staffed by qualified cybersecurity experts known as the Concierge Security team (CST). Arctic Wolf's CST acts as a trusted security advisor for the financial institution's internal IT team. The CST proactively hunts for hidden threats, performs remote forensics analysis of incidents and provides actionable plans to help remediate incidents.
Section 500.11 Third-Party Service Provider Security Policy Third-party service providers shall implement written policies and procedures to ensure security of information systems and non-public information. This includes periodic assessment of third-party service provider risk and adequacy of cybersecurity practices.	Arctic Wolf facilitates compliance by maintaining written policies based on a risk assessment consistent with our SOC II Type 2 compliance certification. Arctic Wolf has strict security policies in place to prevent unauthorized access to SOC tools. Log data is encrypted in transit and at rest.

23 NYCRR 500 Requirement	Arctic Wolf SOC-as-a-Service Capability
Section 500.13 Limitations on Data Retention Support periodic secure disposal of non-public information except when required to be retained by law or regulation.	The AWN CyberSOC™ service supports auto purging of data in retention settings. When combined with a Concierge Security team's active involvement, this assures that data is securely disposed when it outlives its need.
Section 500.14 Training and Monitoring Implement risk-based policies, procedures and controls to monitor activity of authorized users and detect unauthorized access.	Arctic Wolf provides advisory services to audit your firewall and Active Directory configurations. Arctic Wolf can monitor custom domain groups that give access to sensitive datasets.
Section 500.16 Incident Response Plan Establish a written incident response plan for responding to and recovering from cybersecurity events.	Arctic Wolf facilitates incident response plans through its Incident Response Simulation Service that runs through live table-top exercises, makes recommendations on how to rapidly respond to a set of cyberthreats, and addresses regulatory requirements.

About Arctic Wolf

Arctic Wolf provides SOC-as-a-service that is redefining the economics of security. The AWN CyberSOC™ service is anchored by Concierge Security engineers and includes 24×7 monitoring, custom alerting and incident investigation and response. There is no hardware or software to purchase, and the end-to-end service includes a proprietary cloud-based SIEM, threat intelligence subscriptions and all the expertise and tools required. For more information about Arctic Wolf and the AWN CyberSOC, visit https://www.arcticwolf.com.

ARCTIC WOLF

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
info@arcticwolf.com