ConductorOne

How to Comply with the NYDFS Cybersecurity Regulation’s Identity Security Mandates

Cybersecurity threats are constantly evolving, leading regulatory bodies like the New York Department of Financial Services (NYDFS) to issue updates to their cybersecurity requirements. In 2023, the NYDFS finalized an amendment to its cybersecurity regulation, 23 NYCRR Part 500, which mandates that financial institutions safeguard sensitive data and critical systems. This regulation requires organizations to implement risk-based cybersecurity programs, robust access controls, and senior management oversight, and to conduct annual compliance certifications. 23 NYCRR Part 500 is designed to address immediate vulnerabilities and long-term resilience to protect against threats from cybercriminals, nation-states, and other actors.

Part 500 applies to entities regulated by the NYDFS and requires compliance with proactive measures to secure customer data and critical systems. Effective identity and access management is central to these measures. Noncompliance can result in severe penalties, reputational damage, and operational disruptions. For regulated organizations, adhering to these requirements is not just about avoiding penalties; it’s about building trust, ensuring business continuity, and demonstrating proactive risk management.

In this article, you’ll learn about the 23 NYCRR Part 500 compliance standard, with a focus on its impact on identity security.

How Does Implementing 23 NYCRR Part 500 Impact Your Organization?

The importance of Part 500 continues to grow as financial institutions face an escalating number of cyberthreats. High-profile data breaches and sophisticated attacks underscore the need for robust regulations that prioritize protecting sensitive information. According to a recent IBM report, the average cost of a data breach reached $4.88 million in 2024—a 10 percent increase from the previous year—underscoring the significant financial and reputational risks organizations face. Reputational damage can be particularly difficult to recover from.

For identity security programs, Part 500 introduces critical standards that strengthen how organizations govern, manage, and secure access to their systems and data. The regulation emphasizes not just perimeter security but a comprehensive approach to protecting identities, ensuring that only authorized individuals access critical systems, assets, and sensitive information.

Key controls within 23 NYCRR Part 500 relevant to identity security include:

- → **500.4 Chief Information Security Officer:** Cybersecurity governance and the appointment of a CISO to establish leadership accountability.
- → **500.7 Access Privileges:** Enforcing the principle of least privilege to restrict unnecessary access.
- → **500.12 Multi-factor Authentication:** Adding an essential layer of security to prevent unauthorized access.
- → **500.16 Incident Response Plan:** Ensuring timely responses to security events to mitigate damage and prevent escalation.

500.4 Chief Information Security Officer

A key requirement of 23 NYCRR Part 500 is appointing a Chief Information Security Officer (CISO) to oversee cybersecurity programs and manage organizational risk. The CISO ensures cybersecurity policies are not only implemented but also actively monitored and enforced under dedicated leadership. The regulation allows flexibility by permitting organizations to appoint a CISO internally, through an affiliate, or via a third-party service provider, provided that the entity retains accountability and ensures compliance with the regulation’s standards.

The CISO’s role extends beyond oversight; they are responsible for reporting on the cybersecurity program and material risks to the board of directors or a senior officer at least once a year. These reports provide a comprehensive view of cybersecurity policies, risk assessments, and the effectiveness of implemented measures. Additionally, the CISO must assess and report on the organization’s cybersecurity posture, identifying material risks, weaknesses, and the effectiveness of the cybersecurity program. This involves providing a thorough evaluation of potential vulnerabilities and addressing any factors that could lead to a cybersecurity event.

The Part 500 compliance standard places the responsibility for cybersecurity directly with leadership, fostering a proactive and transparent approach to risk management. This requirement ensures accountability starts at the very top of the organization.

500.7 Access Privileges

To comply with 23 NYCRR Part 500, businesses must also restrict access to sensitive information and systems based on the principle of least privilege. Least privilege requires limiting a user's rights and access to only what is necessary for their work, reducing the risk of unauthorized data access, exposure, or misuse. Tools like identity governance and administration (IGA) platforms help enforce least privilege through user access reviews, identity lifecycle management, and just-in-time access. These capabilities ensure permissions stay aligned with current roles and responsibilities while preventing overprovisioning and other risky access. This approach also helps mitigate potential insider threats and reduces the attack surface.

Conducting periodic reviews of access privileges helps detect and address potential risks, such as unnecessary permissions and dormant or overprivileged accounts. Promptly revoking access for employees who have left the organization or whose credentials are compromised is important for preventing unauthorized access and breaches.

500.12 Multi-factor Authentication (MFA)

23 NYCRR Part 500 also requires the use of multi-factor authentication (MFA) to safeguard against unauthorized access. MFA is the first line of defense when passwords get compromised, as it requires users to verify their identity through additional means, such as biometrics, codes generated by authentication apps, or hardware-based mechanisms like YubiKeys, which significantly reduces the likelihood of unauthorized access.

500.12 states that MFA is required for individuals accessing internal networks from outside, unless the CISO approves an alternative control that is either equivalent or more secure. This requirement is primarily focused on privileged users, whose accounts are common targets for cyberattacks because of the level of access they may provide to attackers. MFA policies help prevent data breaches by safeguarding critical systems, which also protects against the reputational and financial damage of cyber incidents. This access control mechanism also maintains business continuity by reducing the risk of operational disruptions when credentials are compromised.

500.16 Incident Response Plan

Timely reporting of cybersecurity events is a fundamental aspect of 23 NYCRR Part 500 that ensures swift action and transparency in the face of potential incidents. Organizations must notify the NYDFS within 72 hours of determining that a cybersecurity event has occurred. Reportable events include those that require notifying regulatory bodies or that could significantly impact the organization's operations. To meet this requirement, organizations need a robust incident response program.

An incident response plan is a structured approach to identifying, managing, and mitigating cybersecurity incidents that typically includes advanced security tools. Some examples of incident response tools include:

- → XDR and EDR platforms, which focus on detecting and responding to threats to endpoints and across systems
- → SOAR platforms, which help automate and orchestrate responses
- → UEBA tools, which analyze user behavior to identify anomalies

Combined with structured processes like real-time monitoring, incident investigation protocols, and predefined response plans, these tools enable organizations to detect suspicious activity, escalate issues through clear procedures, and respond effectively to minimize potential damage.

An incidence response program should include clear procedures for identifying and escalating incidents, as well as timely reporting to NYDFS. An annual compliance statement must also be submitted, certifying adherence to 23 NYCRR Part 500 and documenting any identified areas for improvement and remediation efforts. Moreover, an effective incident detection and response program demonstrates a high level of incident response maturity and reduces regulatory risk while maintaining operational resilience.

Conclusion

Any organization under the jurisdiction of NYDFS needs to be able to navigate the requirements of 23 NYCRR Part 500. This regulation emphasizes key areas such as cybersecurity governance, identity and access management, and incident reporting, providing a framework to address current cybersecurity challenges. The appointment of a CISO, enforcement of least privilege access, and implementation of multifactor authentication are foundational measures for building a strong cybersecurity strategy aligned with this standard.

To meet these challenges effectively, companies need modern tools that simplify identity governance and support compliance efforts. ConductorOne is a modern identity governance platform that simplifies access control, automates governance workflows, and enhances security. It addresses the challenges of managing access across diverse environments by centralizing access visibility and enabling robust access controls, fully automated access reviews, streamlined identity lifecycle management, and just-in-time access provisioning. ConductorOne ensures organizations enforce least privilege, reduce standing privileges, and adopt zero-trust architecture, helping meet compliance requirements such as 23 NYCRR Part 500 while improving efficiency and strengthening overall security.

Talk to our team.

Or take a self-guided tour to learn more!

Try ConductorOne now

Get a demo

ConductorOne

AICPA
SOC