OROCK
TECHNOLOGIES

ORock and Title 23 NYCRR Part 500: NYDFS Cybersecurity Regulation Requirements Supporting Customer Compliance

Table of Contents

Introduction

In today's hyperconnected world, cybersecurity threats carried out by nation-states, terrorist organizations and independent criminal actors continue to escalate and wreak havoc on information and financial systems. In response to destructive cyber-attacks against the financial services industry, the New York State Department of Financial Services (NYDFS) introduced Title 23 NYCRR Part 500, a regulation establishing cybersecurity requirements for financial services companies. This regulation, which took effect on March 1, 2017, is designed to protect customer information and the information technology systems of regulated entities. As a result, financial institutions are now required to assess their specific risk profiles and design a program that mitigates their cybersecurity risks in a robust fashion.

ORock Technologies, Inc. (ORock) is a high-performance hybrid cloud service provider built on OpenStack and certified by FedRAMP and the Department of Defense that provides IT infrastructure and cloud services for secure compute, storage and network operations. ORock serves highly regulated industries and government sectors, helping organizations reduce costs, improve operations and streamline applications when an organization migrates its workloads to our cloud. At ORock, security is of utmost importance and is a shared responsibility between us and our customers. We ensure security of the cloud supporting infrastructure while our customers are responsible for security of their systems built on top of our cloud infrastructure.

This resource provides you with the necessary background on how ORock's security and privacy controls are applied to support financial institutions' compliance with the Title 23 NYCRR Part 500 cybersecurity regulation. A discussion of the following sections from the NYDFS regulation illustrates how we support customer compliance; however, as the covered entity, financial institutions are ultimately responsible for staying in compliance with the regulation:

- Cybersecurity Program - Section 500.2
- Cybersecurity Policy - Section 500.3
- Chief Information Security Officer - Section 500.4
- Penetration Testing and Vulnerability Assessments - Section 500.5
- Audit Trail - Section 500.6
- Access Privileges - Section 500.7
- Application Security - Section 500.8
- Risk Assessment - Section 500.9
- Cybersecurity Personnel and Intelligence - Section 500.10
- Third Party Service Provider Security Policy - Section 500.11
- Multi-Factor Authentication - Section 500.12
- Limitations on Data Retention - Section 500.13
- Training and Monitoring - Section 500.14
- Encryption of Nonpublic Information - Section 500.15
- Incident Response Plan - Section 500.16

Cybersecurity Program - Section 500.2

The NYDFS cybersecurity regulation requires each financial services institution to maintain a cybersecurity program based on assessments of cybersecurity risks and designed to protect the information system. This includes the installment of a robust cybersecurity plan and the initiation and maintenance of an ongoing reporting system for cybersecurity events.

ORock leadership and technology stakeholders are committed to the implementation of robust security and privacy practices. ORock security controls are tailored accordingly so that cost-effective safeguards can be applied commensurate with the risk and sensitivity of the data and system, in accordance with statutory, regulatory, and contractual obligations. ORock participates in numerous audit programs including independent third-party audits to validate adherence and compliance with industry standards and requirements. As a result, the confidentiality, integrity and availability of our cloud supporting infrastructure is always protected, providing a safe environment for our customers' data.

As part of our cybersecurity program, ORock maintains compliance with many industry-recognized certifications and frameworks, some of which are highlighted below.

- FedRAMP: This is a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services. ORock is certified with FedRAMP as a moderate cloud service provider which means our solution comes with 325+ security controls.
- PCI DSS: This is a set of security standards designed to ensure that companies that process, store or transmit credit card data maintain a secure cardholder environment. Our cloud supporting infrastructure is PCI DSS-certified and can be leveraged by customers who want to migrate their cardholder data environment to the cloud.
- HIPAA: HIPAA establishes requirements for the protection and confidential handling of protected health information (PHI), among other requirements. The HIPAA Privacy rule requires health care providers and their business associates to develop and follow procedures that ensure the confidentiality and security of PHI when it is received, processed, transferred or shared. As a business associate, ORock adheres to HIPAA and provides support to customers who must comply with the HIPAA rule.
- HITECH: As an expansion of HIPAA, HITECH has strengthened the privacy and security protections for health information, along with increased penalties for violations of the HIPAA rule. Together, HIPAA and HITECH enforce safeguards related to the use and disclosure of PHI. The ORock cloud supporting infrastructure is compliant with HIPAA and HITECH requirements, making it secure for hosting electronic protected health information.

- DoD IL2: The U.S. Department of Defense (DoD) has defined additional cloud computing security and compliance requirements required of Cloud Service Providers (CSPs) supporting DoD customers. ORock has been granted a DoD Impact Level 2 (IL2) Provisional Authority To Operate (P-ATO) based on our FedRAMP Moderate authorization. Compliance with IL2 P-ATO allows us to host non-controlled, unclassified information as defined by the DoD Cloud Computing Security Requirements Guide (SRG).

To fulfill Title 23 NYCRR Part 500 compliance, financial institutions are responsible for maintaining a cybersecurity program that protects their environments while hosted on our cloud supporting infrastructure.

Cybersecurity Policy - Section 500.3

The NYDFS rule requires institutions to implement and maintain written cybersecurity policies to protect its Information Systems and Nonpublic Information stored on those Information Systems. These policies are required to address cybersecurity subjects, including:

- access controls and identity management;
- asset inventory and device management;
- business continuity and disaster recovery planning and resources;
- systems and network monitoring;
- physical security and environmental controls;
- risk assessment, incident response; and
- vendor and third-party service provider management.

ORock maintains a set of written policies and procedures covering all relevant cybersecurity areas associated with our cloud supporting infrastructure as required by our cybersecurity program. ORock reviews its policies when there is a major change in our environment and at least annually to keep our policies and actions aligned with current industry guidelines, ensuring our cloud supporting infrastructure is adequately protected.

Financial institutions are, in turn, responsible for developing well-documented information security policies, procedures and processes to protect their assets and helping their employees understand critical security issues and best practices that comply with the 23 NYCRR 500 regulation.

Chief Information Security Officer - Section 500.4

The NYDFS rule requires financial institutions to designate a Chief Information Security Officer (CISO) responsible for overseeing the institution’s cybersecurity program and enforcing its cybersecurity policies. The CISO is required to provide written annual reports to the board of directors on the institution’s cybersecurity program and material cybersecurity risks, including the confidentiality of nonpublic information and the integrity and security of its information systems.

ORock has appointed a Chief Security Officer (CSO) with the mission and resources to coordinate, develop, implement and maintain the organization-wide cybersecurity program. This includes overseeing risk assessments and continuous monitoring, and enforcing security policies, procedures and compliance to protect the security of the cloud supporting infrastructure. The CSO acts in coordination with the Chief Operating Officer (COO) for operationally-related security activities.

The financial institution's designated CISO is responsible for all aspects of information security in their system environment. The CISO must manage issues relating to the institution's information security and cybersecurity posture and must provide written annual reports to meet the requirements set forth in the NYDFS rule.

Penetration Testing and Vulnerability Assessments - Section 500.5

Financial institutions are required to incorporate monitoring and testing designed to assess the effectiveness of its cybersecurity program through continuous monitoring or periodic penetration testing and vulnerability assessments.

ORock has implemented a continuous monitoring strategy that encompasses vulnerability scanning, annual security assessments, flaw remediation processes, periodic security reauthorization, annual penetration testing and continuous network monitoring for the ORock cloud supporting infrastructure. In addition to these explicit processes, ORock reviews and updates associated security documentation at least annually to ensure accuracy and compliance. ORock has implemented this strategy in accordance with timelines dictated by our cybersecurity program.

Financial institutions are responsible for having their own continuous monitoring process where relevant controls are assessed and enhancements are made, if necessary. To meet the 23 NYCRR 500 requirement, financial institutions must perform penetration testing and vulnerability assessments in their environment if no credible continuous monitoring initiatives are available.

Audit Trail - Section 500.6

The NYDFS rule requires institutions to maintain systems that can reconstruct material financial transactions and include audit trails designed to detect and respond to cybersecurity events that are likely to impact normal operations.

Auditing is an integral security aspect at ORock that ensures consistent and reliable accountability within the cloud supporting infrastructure. Security audit functions are coordinated with organizational entities requiring audit-related information to enhance mutual support and guide the selection of relevant auditable events. In addition, we ensure that auditable events are supported with a rationale in order to be considered adequate for after-the-fact investigations of security incidents. ORock ensures that processes are in place to audit additional events continuously, based on current threat information and ongoing risk assessment. For retention requirements, audit logs can be configured by the customer within their environment and retained for as long as required in accordance with the NYDFS rule.

Financial institutions must define baseline events that are to be captured within their environment and ensure that such events are being captured and sent to a stand-alone log server for analysis and storage for the required amount of time to meet 23 NYCRR 500 requirements.

Access Privileges - Section 500.7

According to the NYDFS rule, financial institutions must limit user access privileges to information systems that contain nonpublic information.

ORock closely restricts access to the cloud supporting infrastructure and only authorizes direct access for a small subset of appropriately screened and experienced personnel. ORock personnel authorized to access the cloud supporting infrastructure are identified and authenticated uniquely using PKI authentication with smart cards and a hardware reader solution for multi-factor authentication. The PKI solution is closely integrated with the LDAP system, and access to the VPN interface is limited to those authorized personnel with an administrator account present in the LDAP. Privileged administrator accounts are limited to the personnel who are authorized by role and responsible for performing day-to-day maintenance, operations and monitoring of the cloud supporting infrastructure.

Financial institutions must limit user access privileges in their environment by assigning well-defined roles and authorizing the minimum access necessary for their users to accomplish assigned responsibilities.

Application Security - Section 500.8

The NYDFS rule requires financial institutions to include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications, and procedures for evaluating, assessing and testing the security of externally developed applications.

ORock does not develop applications in-house. For services provided by externally developed applications, ORock performs a security review of any products or services being introduced into the ORock cloud supporting infrastructure. As part of the security review, we validate that security functionality, strength and assurance requirements and criteria are in place. If the product is an external information system that is implemented outside the FedRAMP system boundary, the security review also includes a risk assessment that is conducted in accordance with NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments. Security reviews are completed for any introduction of hardware or software into the system boundary, as well as before any significant changes (major releases, adding new hardware, etc.) that will adversely affect the integrity of the system's FedRAMP authorization.

Financial institutions should have a documented, formalized Systems or Software Development Life Cycle (SDLC) process in place. This includes having SDLC policies and procedures, the use of change control processes, using source code tools, performing code reviews and other related items as needed in their environment to meet requirements set forth in the NYDFS rule.

Risk Assessment - Section 500.9

A key requirement of the NYDFS rule is conducting periodic risk assessments in accordance with written policies and procedures for use in designing the cybersecurity programs for financial institutions.

ORock has employed a risk assessment program to evaluate the ongoing effectiveness of security controls applied in our cloud supporting infrastructure. ORock uses an independent Third-Party Assessment Organization (3PAO) to perform assessments on the ORock environment in accordance with requirements of our cybersecurity program. These risk assessments evaluate the confidentiality, integrity, security and availability of the cloud supporting infrastructure and hosted nonpublic information and review the adequacy of existing controls. Risks identified at the end of the assessment are tracked in our flaw remediation processes until they are remediated within timelines defined by our cybersecurity program. ORock conducts risk assessments on an annual basis in accordance with the continuous monitoring and re-assessment requirements of our cybersecurity program.

Financial institutions are responsible for putting together risk assessment policies and procedures and undergoing annual security risk assessments tailored to their environment to document the security posture including strengths, weaknesses and risks, as required by the NYDFS rule.

Cybersecurity Personnel and Intelligence - Section 500.10

Financial institutions are required to use qualified cybersecurity personnel to manage cybersecurity risks and to oversee the performance of the core cybersecurity functions. Cybersecurity personnel are also required to be trained and take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

All ORock personnel are screened according to their intended role and are subject to background checks prior to onboarding for employment with ORock. ORock hires only U.S.-persons; all employees and contractors undergo basic security awareness training as well as role-based training at the time of hire and annually thereafter. Additionally, key cybersecurity personnel maintain current knowledge of changing threats and countermeasures through subscriptions to U.S.-CERT, industry security newsletters, subscription lists and patch update news releases. ORock responds to security events identified in industry security newsletters which are implemented according to the threat or flaw risk categorization. Customers can rest assured that their nonpublic data will stay confidential and intact.

Financial institutions should have competent and well-trained cybersecurity personnel on board and provide personnel with annual security awareness and role-based cybersecurity training applicable to their expertise, in accordance with the NYDFS rule.

Third-Party Service Provider Security Policy - Section 500.11

The NYDFS rule states that financial institutions must implement written policies and procedures designed to safeguard the security of information systems and nonpublic information that are accessible to, or held by, Third-Party Service Providers. Such policies and procedures are to be based on the risk assessment of the covered entity and shall address to the extent applicable:

- the identification and risk assessment;
- minimum cybersecurity practices required;
- due diligence processes used to evaluate the adequacy of cybersecurity practices;
- periodic assessments based on the risk they present and the continued adequacy of their cybersecurity practices.

In addition, the policies and procedures are expected to include relevant guidelines for due diligence and/or contractual protections addressing:

- the third party's use of access controls including multi-factor authentication;
- the third party's use of encryption;
- notice required to be provided to the institution for cybersecurity events directly impacting the institution or the information held by the third party on behalf of the institution; and
- representations and warranties addressing the third-party service provider's cybersecurity policies.

ORock employs third-party providers that oversee and maintain third-party use policies and procedures to ensure efficient safety of the cloud supporting infrastructure. In relation to the 23 NYCRR 500 program, ORock operates as a third-party service provider to financial institutions and implements cybersecurity practices and risk assessments that consistently provide adequate protection for our financial institution customers. The following areas are specifically addressed in support of the 23 NYCRR 500 third-party requirements:

- Multi-factor authentication: This is implemented for all users with access to our cloud supporting infrastructure.

- Encryption: Our cloud supporting infrastructure employs FIPS-validated cryptography for protection of data at rest and information in transmission. Trusted certificate authorities (CAs) that are leveraged employ FIPS-validated cryptographic modules to control and protect root certificates.

- Cybersecurity events notices: ORock personnel are trained to immediately report suspected or potential security events identified during daily activities. Personnel report suspected security incidents to the

Security Operations Center (SOC). The SOC notifies the ORock COO and CSO of the security incident status and any exploited vulnerabilities as the incident is being triaged and resolved. ORock requires personnel to report suspected security incidents within the timelines specified in the 23 NYCRR 500 requirements as well as in NIST SP-800-61 as part of our cybersecurity program.

Financial institutions are responsible for having implemented comprehensive vendor management policies, procedures and practices for all relevant third-parties being used by the institution. The financial services institution is ultimately responsible for performing the necessary initial and ongoing due diligence measures on contracted third-parties in compliance with 23 NYCRR 500 cybersecurity requirements.

Multi-Factor Authentication - Section 500.12

In order to protect financial services against unauthorized access to nonpublic information or information systems, any individual accessing the institution's internal networks from an external network is required to use multi-factor authentication, unless otherwise approved in writing.

Personnel authorized to access the cloud supporting infrastructure are considered privileged users, and by default, ORock implements multi-factor authentication for all privileged users. In addition, the systems used in the production environment require multi-factor authentication for remote access. In order to successfully authenticate to the cloud supporting infrastructure, authorized personnel use their individual PIN with the certificate stored on their smart card. ORock's multi-factor authentication measures are FIPS 140-2 validated and comply with NIST SP800-63B guidance in line with our cybersecurity program.

To prevent unauthorized access to nonpublic data, financial institutions are responsible for implementing a two-factor or multi-factor authentication solution for user access to their systems that are hosted on our cloud.

Limitations on Data Retention - Section 500.13

The NYDFS rule requires financial institutions to include policies and procedures for the secure disposal, on a periodic basis, of any nonpublic information that is no longer necessary for business operations. The exceptions include when such information is otherwise required to be retained by law or regulation, and when targeted disposal is not reasonably feasible due to the way the information is maintained.

ORock coordinates with customers on data retention needs when a customer notifies us they are closing their account. ORock's retention requirements associated with customer data ends with the expiration of the customer's contract with us. The logs associated with the environment are retained in accordance with our retention policies.

Financial institutions are responsible for maintaining documented policies, procedures and processes regarding data retention and disposal, including information on the types of data stored, how the data is stored, for how long the data is stored and what data removal and destruction procedures are in place for purging data from the institution’s systems.

Training and Monitoring - Section 500.14

The NYDFS rule requires financial institutions to implement risk-based policies, procedures and controls to monitor the activity of authorized users and to detect unauthorized access, use or tampering with nonpublic information by authorized users. In addition, institutions need to provide regular cybersecurity awareness training for all personnel.

Personnel authorized to access the cloud supporting infrastructure are considered privileged users and are monitored in a consistent fashion. ORock uses a SIEM tool to collect event logs from information system components and monitors system use, security events and activities to detect and investigate security breaches, system abuse and other events of interest. Account usage is logged and monitored, and event logs are used to explicitly capture privileged user actions and the execution of privileged functions. ORock employees and contractors are required to take basic security awareness training, inclusive of an insider threat component, upon onboarding. In the event of a change to the ORock offering, applicable personnel will take relevant security awareness training to ensure personnel are adequately trained. ORock employees and contractors take basic security awareness training and role-based security training on an annual basis.

As a financial institution, you must ensure that measures are in place for audit logging and monitoring of your authorized users’ activity. You are also responsible for personnel cybersecurity training in order to remain in compliance with 23 NYCRR 500 requirements.

Encryption of Nonpublic Information - Section 500.15

Financial institutions are required to implement controls, including encryption, to protect nonpublic information held or transmitted by the institution both in transit over external networks and at rest. To the extent encryption is not feasible, the institution is allowed to secure this information using compensating controls and conduct annual reviews.

ORock employs FIPS-validated cryptography for protection of data at rest and information in transmission. For external network traffic, ORock enforces TLS encryption by redirecting HTTP requests, and only permitting inbound communication via HTTPS. In addition, ORock relies on a trusted CA for external SSL certificates. Trusted CAs that are leveraged employ FIPS-validated cryptographic modules to control and protect root certificates.

Financial institutions are responsible for using approved encryption protocols to transmit or store data while hosted on our cloud for their 23 NYCRR 500 compliance.

Incident Response Plan - Section 500.16

The NYDFS rule requires financial institutions, as part of their cybersecurity programs, to establish written incident response plans designed to promptly respond to and recover from cybersecurity events affecting the confidentiality, integrity or availability of the institution's information systems or their operations.

ORock has developed a security Incident Response Plan to serve as the guiding document and process definition for information security incident response, monitoring and reporting activities within the cloud supporting infrastructure. ORock incident response personnel review the incident response plan at least annually and remain current on incident response documentation. ORock has implemented an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication and recovery.

Financial institutions must put in place a well-documented incident response plan for their environment. This must include processes for reporting and recovering from specified cybersecurity events in order to meet their 23 NYCRR 500 compliance requirements.

Summary

Meeting the NYDFS cybersecurity regulation is a priority for financial institutions operating in New York state. To remain in compliance with this regulation, financial institutions need to assess whether introducing a cloud component accelerates or hinders their compliance initiative. Hosting your system on the ORock cloud platform provides the secure, compliant underlying cloud infrastructure that complements your cybersecurity program in support of your 23 NYCRR 500 obligation as a financial institution. We continually test and enhance the security of our cloud supporting infrastructure and are committed to helping protect the confidentiality, integrity and availability of customer data. Our approach supports financial institutions and their efforts to meet 23 NYCRR 500's most challenging requirements by providing complete security of the underlying cloud supporting infrastructure. This allows institutions who are responsible for maintaining security within their own environment to meet compliance needs and reduce associated cybersecurity threats.

For additional information, contact an ORock sales representative.

571.386.0201 | sales@orocktech.com | www.orocktech.com