Compliance Brief

Data Security Compliance

With the NYDFS Cybersecurity Requirements for Financial Services

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

What is the NYDFS Cybersecurity Requirements for Financial Services Companies?

The New York State Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies, or 23 NYCRR Part 500 regulation, requires that regulated institutions implement, maintain, and annually certify that they have cybersecurity programs in place to protect the integrity of their information systems and customers' data.

The regulation promotes the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously, be responsible for the organization's cybersecurity program, and file an annual certification confirming compliance with these regulations.

Which companies are supervised by the NYDFS?

Any institution that needs a license, registration, or charter from the New York State Department of Financial Services is regulated by the NYDFS. Examples of covered entities include state-chartered banks, foreign banks licensed to operate in the state of New York, licensed lenders, private bankers, savings and loans associations, mortgage companies, insurance companies, and other financial service providers.

When did the NYDFS Cybersecurity Requirements go into effect?

The initial phase of the New York State Cybersecurity Requirements for Financial Services Companies took effect on March 1, 2017. However, the entirety of the requirements was only enforced two years later, by March 1, 2019.

What are the penalties for NYDFS Cybersecurity Requirements non-compliance?

Under NY Banking Law, the NYDFS penalties start at $2,500 a day for each day of noncompliance with NYDFS Part 500. If noncompliance is determined to be a "pattern" by the NYDFS superintendent, the fine may increase to $15,000 a day. If the superintendent decides that any violations have been committed "knowingly and willfully," the fine will jump to $75,000 daily. Recent 2022 enforcement actions imposed monetary penalties in the $4.5 million to$5million range.

How can Thales help with NYDFS Cybersecurity Requirements compliance?

Thales helps organizations comply with the NYDFS Cybersecurity Requirements by assessing risk, managing access, and protecting data at rest and in-motion.

NYCRR Part 500: Cybersecurity Requirements for Financial Services Companies

This regulation requires each company to assess its specific risk profile and design, implement, maintain, and annually certify a cybersecurity program that addresses its risks and protects customer information as well as information technology systems.

Thales helps organizations by:

- Providing a complete audit trail
- Managing and monitoring access privileges
- Securing development of applications
- Assessing risk
- Managing third party service provider risk
- Providing multi-factor authentication
- Encrypting non-public information

How Thales solutions help with NYDFS Compliance

NYDFS Part 500	Requirement	Thales Solutions
500.06	"...**include audit trails** designed to detect and respond to cybersecurity events."	**Thales Data Security Solutions** maintain extensive access logs and prevent unauthorized access. In particular, CipherTrust Transparent Encryption security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and external SIEM systems. **SafeNet Trusted Access** allows organizations to respond to and mitigate the risk of data breach by providing an immediate, up to date audit trail of all access events to all systems. Automated reports document all aspects of access enforcement and authentication. In addition, the service automatically streams logs to external SIEM systems.
500.14	"...**monitor and log the activity** of authorized users and **detect unauthorized access.**"	
500.07	"...**limit user access privileges** to Information Systems."	**Thales OneWelcome Identity & Access Management** products and solutions limit the access of internal and external users based on their roles and context. Strong multi-factor authentication (MFA), granular access policies, and fine-grained authorization policies help ensure the right user is granted access to the right resource at the right time. This minimizes the risk of unauthorized access. **CipherTrust Transparent Encryption** encrypts sensitive data and enforces granular privileged-user-access management policies that can be applied by user, process, file type, time of day, and other parameters. It provides complete separation of roles enabling only authorized users and processes can view unencrypted data.
500.08	"...ensure the use of **secure development practices for in-house developed applications** utilized by the Covered Entity..."	**CipherTrust Platform Community Edition** makes it easy for DevSecOps to deploy data protection controls in hybrid and multi-cloud applications. The solution includes licenses for CipherTrust Manager Community Edition, Data Protection Gateway, and CipherTrust Transparent Encryption for Kubernetes. **CipherTrust Secrets Management** is a state-of-the-art secrets management solution, which protects and automates access to secrets across DevOps tools and cloud workloads including secrets, credentials, certificates, API keys, and tokens. **Thales Data Protection on Demand (DPoD)** is a cloud-based marketplace that offers Luna hardware security modules HSMs and CipherTrust solutions as a service. This enables in-house teams to leverage these proven and certified data security solutions easily and securely in their own offerings.
500.09	"...conduct a periodic **Risk Assessment** of the Covered Entity's Information Systems."	**CipherTrust Data Discovery and Classification** identifies structured and unstructured sensitive data on-premises and in the cloud. Built-in templates enable rapid identification of regulated data, highlight security risks, and help uncover compliance gaps.
500.11	"...ensure the security of Information Systems and **Nonpublic Information that are accessible to, or held by, Third Party Service Providers."**	**CipherTrust Cloud Key Manager** can reduce third party risks by maintaining on-premises under the full control of the financial institution the keys that protect sensitive data hosted by third party cloud providers. This increases operational efficiency through harmonization and automation. **CipherTrust Transparent Encryption** provides complete separation of administrative roles, so only authorized users and processes can view unencrypted data. Sensitive data stored in a third-party cloud will not be accessible in cleartext to unauthorized users. These could include third party cloud provider employees, such as support engineers, DB admins, or potentially malicious processes. In addition, Thales Portfolio of Data Security solutions offer the most comprehensive range of data protection for cloud environments. **Thales Data Protection on Demand (DPoD)** provides built in high availability and backup to its **cloud-based Luna Cloud HSM and CipherTrust Key Management services**, to the **High Speed Encryption** appliances that secures data moving between clouds, to on-premises locations, or to third parties.

How Thales solutions help with NYDFS Compliance

NYDFS Part 500	Requirement	Thales Solutions
500.12	"...shall use effective controls, which may include **Multi-Factor Authentication.**"	**SafeNet Trusted Access** provides commercial, off-the-shelf multi-factor authentication with the broadest range of hardware and software authentication methods and form factors. This allows customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally-managed policies — all managed from one authentication back-end delivered in the cloud or on-premises.
500.15	"...**Implement controls, including encryption**, to protect Nonpublic Information held or transmitted by the Covered Entity both **in transit over external networks and at rest.**"	**CipherTrust Data Security Platform** provides multiple capabilities for protecting data at rest in files, volumes, and databases. Among them: • **CipherTrust Transparent Encryption** delivers data-at-rest encryption with centralized key management and privileged user access control. This protects data wherever it resides, on-premises, across multiple clouds, and within big data and container environments. • **CipherTrust Tokenization** permits the pseudonymization of sensitive information in databases while maintaining the ability to analyze aggregate data without exposing sensitive data during the analysis or in reports. • **CipherTrust Enterprise Key Management** streamlines and strengthens key management in cloud and enterprise environments over a diverse set of use cases. Leveraging FIPS 140-2-compliant virtual or hardware appliances, Thales key management tools and solutions deliver high security to sensitive environments and centralize key management for home-grown encryption, as well as third-party applications. **Thales Luna Hardware Security Modules (HSMs)** protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Luna HSMs are available on-premises, in the cloud as-a-service, and across hybrid environments. • Generates and protects root and certificate authority (CA) keys, providing support for PKIs across a variety of use cases. • Signs application code to ensure software remains secure, unaltered, and authentic. • Creates digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other network deployments. **Thales High Speed Encryptors (HSEs)** provide network-independent data-in-motion encryption (layers 2, 3, and 4) ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back. Our network encryption solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception — without performance compromise. Thales HSEs are available as both physical and virtual appliances, supporting a wide spectrum of network speeds from 10 Mbps to 100 Gbps.

About Thales

As the global leader in data security, Thales helps the most trusted brands and organizations around the world protect their most sensitive data and software, secure the cloud, provide seamless digital experiences, and achieve compliance through our industry-leading data encryption, identity and access management, and software licensing solutions.

cpl.thalesgroup.com

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us