DataKeep™

SecurityFirst™ Protecting Critical Data

New York State
Department of Financial Services

Compliance Bulletin
23 NYCRR 500

The New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500) went into effect March 1, 2019 and defines new cybersecurity requirements for all regulated financial institutions around privacy and protection of certain types of collected information and data, and associated penalties for non-compliance .

The new cybersecurity rules 23 NYCRR 500 imposes on regulated organizations include creating a detailed cybersecurity plan with supporting policies, designating a Chief Information Security Officer (CISO) or equivalent role, and the initiation and maintenance of an ongoing reporting system for cybersecurity events. Effectively, executive management holds responsibility for adhering to the regulation and must perform an annual certification confirming compliance.

This regulation does not just focus on protecting personal privacy, but also requires protection of business related information the regulated institution stores, as well as certain personal health information. An organization's answer to this and other compliance mandates will most likely be comprised of documented processes along with software products and services to address the various requirements. There are 23 sections in the 23 NYCRR 500 that detail the requirements. While some requirements are more process oriented, such as designating the CISO role, several center around protecting critical data assets. This document outlines those key areas and highlights how a data-centric solution, such as DataKeep, facilitates compliance.

Fig. 1 - 23 NYCRR 500 Requirements

Section	Title	DataKeep Supports
500.00	Introduction	
500.01	Definitions	
500.02	**Cybersecurity Program**	**YES**
500.03	Cybersecurity Policy	
500.04	Chief Information Security Officer	
500.05	Penetration Testing and Vulnerability Assessments	
500.06	**Audit Trail**	**YES**
500.07	**Access Privileges**	**YES**
500.08	Application Security	
500.09	Risk Assessment	
500.10	Cybersecurity Personnel and Intelligence	
500.11	Third Party Service Provider Security Policy	
500.12	Multi-Factor Authentication	
500.13	**Limitations on Data Retention**	**YES**
500.14	**Training and Monitoring**	**YES**
500.15	**Encryption of Nonpublic Information**	**YES**
500.16	Incident Response Plan	
500.17	Notices to Superintendent	
500.18	Confidentiality	
500.19	Exemptions	
500.20	Enforcement	
500.21	Effective date	

Key Sections Related to Data-centric Protection

500.01 Definitions

(b) Authorized User means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

(d) Cybersecurity Event means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such information System.

(g) Nonpublic Information shall mean all electronic information that is not Publicly Available Information and is:

(1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;

(2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;

(3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

500.02 Cybersecurity Program

(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

500.02 DataKeep for Cybersecurity Program

DataKeep addresses the most stringent compliance requirements across all industries with built-in data protection, data access processes, cryptographic policy enforcement, auditing and reporting capabilities, and integrated key management. DataKeep easily fits into existing security infrastructures, whether as a separate single-pane-of glass, or integrated into automation via REST API. DataKeep provides the ability for customers to implement data access policies that protect encrypted data from unauthorized access, use or other malicious acts.

500.06 Audit Trail

(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

(2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

(b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.

500.06 DataKeep for Audit Trail

DataKeep provides the ability for customers to implement data access policies that protect encrypted data from unauthorized access, use or other malicious acts. In addition, it allows customers the flexibility to log data access events, whether permitted or denied for detection of potential harmful events. These events are logged in real-time, and can be exported to Security Information & Event Management (SIEM) systems for auditing and alerts. DataKeep supports several standard output formats such as Log Event Extended Format (LEEF), Common Event Format (CEF) and Cloud Auditing Data Federation (CADF) for easy integration. This combination of DataKeep and SIEM products can make it possible to shorten the detection cycle, reducing the risk of data compromise.

500.07 Access Privileges

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

500.07 DataKeep for Access Privileges

DataKeep provides the ability for customers to implement role-based access control, privileged access management and separation of security vs. administrative duties to prevent any one person or service provider from having complete system control. Working with your existing directory services, Role-based access controls allow an administrator to define a second layer of data access control policies used to specify which filesystem functions (read, write, etc.), are authorized. Using a Least Privileged Access (LPA) approach, DataKeep automatically denies access to all users unless they have been specifically granted permissions. In addition, Privileged Access Management restrictions can be enforced to prevent system administrators and root users from seeing clear text data. By default, DataKeep creates two distinct roles – Product and Security Administrators. The Product Administrator role deploys the software and monitors the general health of the DataKeep system and all deployed agents. This role has no visibility into policy definitions, agent configurations, deployments or policy logs. The Security Administrator role determines and approves data access rights, manages keys, defines policies, sets logging parameters, and creates the multi-security administrator approval process.

500.13 Limitations on Data Retention

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information identified in section 500.01(g)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

500.13 DataKeep for Limitations on Data Retention

With its transparent, built-in key management capabilities, all phases of key lifecycle stay in your control. Automated key creation, rotation, and revocation/shred conform to industry compliance requirements. When data is no longer required, the customer can revoke the encryption key from the DataKeep system, leaving the data encrypted wherever it is stored, without the key ever being available again for decryption.

500.14 Training and Monitoring

As part of its cybersecurity program, each Covered Entity shall: (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users;

500.14 DataKeep for Training and Monitoring

DataKeep provides the ability for customers to implement data access policies that protect encrypted data from unauthorized access, use or other malicious acts. In addition, it allows customers the flexibility to log data access events, whether permitted or denied for detection of potential harmful events. These events are logged in real-time, and can be exported to Security Information & Event Management (SIEM) systems for auditing and alerts.

500.15 Encryption of Nonpublic Information

(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

500.15 DataKeep for Encryption of Nonpublic Information

DataKeep allows customers to deploy agents that encrypt data at the volume-level or for additional granularity, at file-level. The volume encryption agent is a virtual block device that once installed is mounted to look like an attached disk. The file encryption agent works at the file-level based upon fine-grained file or directory level policies. This allows for cryptographic security based upon User, Group or Process, as well as the ability to encrypt the data in place.

DataKeep agents operate at the kernel level of the protected servers for optimal performance. Encryption is transparently applied during file write operations without any end user interaction or noticeable performance degradation.

DataKeep assures confidentiality, data privacy and protection against brute force attacks. The SPxCore™ technology combines cryptographic splitting with AES-256 certified encryption and internal key management certified by the National Institute of Standards and Technology (NIST) to be FIPS 140-2 compliant. DataKeep also takes full advantage of the AES-NI hardware acceleration available in most current processors for optimal performance.

500.22 Transitional Periods

(b) The following provisions shall include additional transitional periods. Covered Entities shall have:

(1) One year from the effective date of this Part to comply with the requirements of sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b) of this Part.

(2) Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06, 500.08, 500.13, 500.14 (a) and 500.15 of this Part.

500.22 DataKeep for Transitional Periods

The key sections that DataKeep will support, are Sections 500.06 (Audit Trail), 500.07 (Access Privileges), 500.13 (Data Retention) and 500.15 (Encryption). These requirements must be supported by September 1, 2018, eighteen months after the effective date, March 1, 2017.

Note that Section 500.07, which covers basic access privileges needs to be in place by the effective date, but the combination of DataKeep policies, encryption and access logging will build upon and strengthen any existing access management once implemented.

DataKeep addresses several key requirements in 23 NYCRR 500 and helps financial institutions ensure their data is protected and private in alignment with the regulation.

SecurityFirst™ delivers advanced security solutions that build a firewall around your data to protect against ever increasing threats and to aid in meeting regulatory requirements such as GDPR, HIPAA, NYCRR and many others.

DataKeep™, our flagship product, serves as your data firewall by using advanced encryption, scalable hierarchical key management, extensive policy enforcement and monitoring of unauthorized access to deliver the highest levels of availability, resiliency and time to value. Security requires a layered approach and protection of the data itself is your last line of defense.

SecurityFirst™
Protecting Critical Data

For a product demonstration or more information contact:
sales@securityfirstcorp.com
888-884-7152
securityfirstcorp.com