SecurityFirst
Protecting Critical Data

DataKeep™

Supporting the Data Protection requirements for NY DFS

New York Department of Financial Services Cybersecurity Regulation 23 NYCRR 500

23 NYCRR 500 went into full effect March 1, 2019 for financial institutions regulated under the state Banking, Insurance or Financial Services Laws. It established new cybersecurity requirements around the privacy and protection of collected and stored personal information as well as business related information and certain personal health information. 23 NYCRR 500 specifically states that technology such as multi-factor authentication and encryption shall be required to safeguard nonpublic information.

23 NYCRR 500 imposes rules that 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 ongoing penetration testing, data protection, encryption and reporting of cybersecurity events. There are 23 sections in 23 NYCRR 500 that detail cybersecurity requirements and the key requirements are listed in the following table.

Section	Title
500.01	Definitions
500.02	Cybersecurity Program
500.03	Cybersecurity Policy
500.04	Chief Information Security Officer
500.05	Pen Testing and Vulnerability Assessments
500.06	Audit Trail
500.07	Access Privileges
500.08	Application Security
500.09	Risk Assessment
500.10	Cybersecurity Personnel and Intelligence

Section	Title
500.11	3rd Party Service Provider Security Policy
500.12	Multi-Factor Authentication
500.13	Limitations on Data Retention
500.14	Training and Monitoring
500.15	Encryption of Nonpublic Information
500.16	Incident Response Plan
500.17	Notices to Superintendent
500.18	Confidentiality
500.19	Exemptions
500.20	Enforcement

How DataKeep from SecurityFirst helps support 23 NYCRR 500

DataKeep's easy-to-use, agent-based deployment model helps protect sensitive data-at-rest wherever it resides -- server managed storage, network file systems or in object storage. It provides a broad range of protection that includes data access management, integrated key management, sophisticated encryption and event logging, that combine to deliver the scalability and flexibility to help protect the most sensitive workloads. DataKeep provides the following capabilities to support California data protection requirements.

- Encrypt personal data
- Manage access to personal data (by role or process)
- Audit data access requests / denials for encrypted personal data
- Provide data erasure through cryptographic shredding

23 NYCRR 500 consists of many definitions and requirements outside the scope of what a data-centric solution like DataKeep can impact. We will focus on specific sections related to data protection. The following table presents areas where SecurityFirst DataKeep can help support 23 NYCRR 500.

Section	Brief Description	Policy	Log/Audit	Encryption
500.02	Use defensive infrastructure, policies and procedures to protect the Nonpublic Information (NPI) stored from unauthorized access, use or other malicious acts	✓	✓	✓
500.06	Use audit trails designed to detect and respond to Cybersecurity Events and maintain certain records up to five years		✓	✓
500.07	Limit user access privileges to Information Systems that provide access to NPI and periodically review such access privileges.	✓	✓	✓
500.13	Include policies and procedures for the secure disposal of any NPI that is no longer necessary for business operations or other legitimate business purposes	✓	✓	✓
500.14	Implement risk-based policies, procedures and controls to monitor the activity of Authorized Users and detect unauthorized access or use of or tampering with NPI.	✓	✓	✓
500.15	Implement controls, including encryption, to protect NPI held or transmitted by the Covered Entity both in transit over external networks and at rest.	✓		✓

The regulation requires each company to assess its specific risk profile and design a program that addresses those risks. It requires that senior management be responsible for the organization's cybersecurity program and file an annual certification confirming compliance. DataKeep encryption and access policies can help meet the specific requirements for implementing and maintaining data privacy and security compliance requirements.

FOR MORE INFORMATION PLEASE VISIT THE SECURITYFIRST DATAKEEP WEBPAGE

About SecurityFirst™

SecurityFirst delivers data-centric solutions that address the high-profile cyber threats facing organizations today, such as data breaches, ransomware and cloud security. We emphasize protection of the data itself to serve as your last line of defense. Data is always protected no matter where it resides and recoverable in the event of an unexpected failure or malicious attack. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure.