PKWARE | SMARTCRYPT

MEET NEW YORK'S FINANCIAL SERVICES CYBERSECURITY REQUIREMENTS WITH SMARTCRYPT

WHAT IS 23 NYCRR 500?

23 NYCRR 500 is a new set of cybersecurity requirements that apply to organizations licensed by the New York State Department of Financial Services. The requirements take a broader approach to cybersecurity than any previous US law, establishing minimum standards for a wide range of security activities, including risk assessment, policy creation, access control, data protection, and event reporting.

From its effective date of March 1, 2017, the law provides four separate transitional periods for organizations to bring their cybersecurity practices into compliance. The first transitional period ended after 180 days, while the final period ends two years from the law's effective date.

HOW DOES 23 NYCRR 500 AFFECT MY ORGANIZATION?

With a few exceptions for smaller organizations, the law applies to all banks, investment companies, and other financial services firms that do business in New York, whether the organizations are based in New York or elsewhere. Covered entities will need to certify once per year that they have met the requirements, including all of the following:

- Establish a formal cybersecurity program and document cybersecurity policies
- Conduct regular risk assessments
- Ensure the security of their applications
- Implement data protection methods including encryption
- Use appropriate controls to limit access to sensitive information
- Notify the New York DFS within 72 hours of a cybersecurity event

In addition, the law indirectly establishes rules for third party service providers that have access to covered entities' nonpublic information. Covered organizations are required to develop third party security policies that will effectively apply many 23 NYCRR 500 mandates to service providers who are not licensed by the New York DFS.

HOW DOES SMARTCRYPT HELP MEET 23 NYCRR 500 REQUIREMENTS?

PKWARE's Smartcrypt combines intelligent data discovery, classification, and data protection to enable enterprise-wide control over sensitive data. With Smartcrypt, financial services organizations and their third party service providers can improve their data security while ensuring compliance with 23 NYCRR 500 and other government and industry mandates.

23 NYCRR 500 REQUIREMENT	SMARTCRYPT SOLUTION
RISK ASSESSMENT (SECTION 500.09)	In order to protect its data, an organization must first understand how much information it has and where the information is located. Smartcrypt's data discovery tools enable organizations to detect sensitive information on end user devices and in network storage locations. Discovery agents can be configured to detect data based on each organization's unique needs and business processes.
ENCRYPTION OF NONPUBLIC INFORMATION (SECTION 500.15)	Smartcrypt applies strong data-level encryption to sensitive information, ensuring that the data remains inaccessible to unauthorized users, even if stolen or mishandled. With simplified key management and cross-platform operability, Smartcrypt is the only solution that facilitates true enterprise-wide encryption.
APPLICATION SECURITY (SECTION 500.08)	Smartcrypt Application Encryption, PKWARE's software development kit, allows organizations to incorporate strong encryption into their existing applications with only a few additional lines of code. Encryption can be applied to structured and unstructured data.
AUDIT TRAILS AND ACTIVITY MONITORING (SECTION 500.06 & 500.14)	Smartcrypt's web-based manager console facilitates complete administrative control over encrypted information. Access control lists determine who is authorized to decrypt protected information, while Smartcrypt's Data Security Intelligence tools provide full reporting on every encryption and decryption operation.
THIRD PARTY SECURITY POLICIES (SECTION 500.11)	Smartkey technology allows organizations to exchange sensitive information with third parties securely and easily. Third-party access privileges can be granted or revoked at any time without the need for re-encryption.
LIMITATIONS ON DATA RETENTION (SECTION 500.13)	Smartcrypt takes policy-based actions on files across the entire enterprise. By using Smartcrypt's data discovery and classification capabilities, organizations can define deletion criteria and automatically delete files that are no longer needed.

PKWARE®

www.PKWARE.com

PKWARE provides a data-centric audit and protection platform that automates policy-driven discovery, classification, and encryption wherever sensitive data is used, shared, or stored.

CORPORATE HEADQUARTERS
201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204

+ 1 866 583 1795

EMEA HEADQUARTERS
79 College Road
Suite 221
Harrow HA1 1BD

+ 44 (0) 203 367 2249