PKWARE

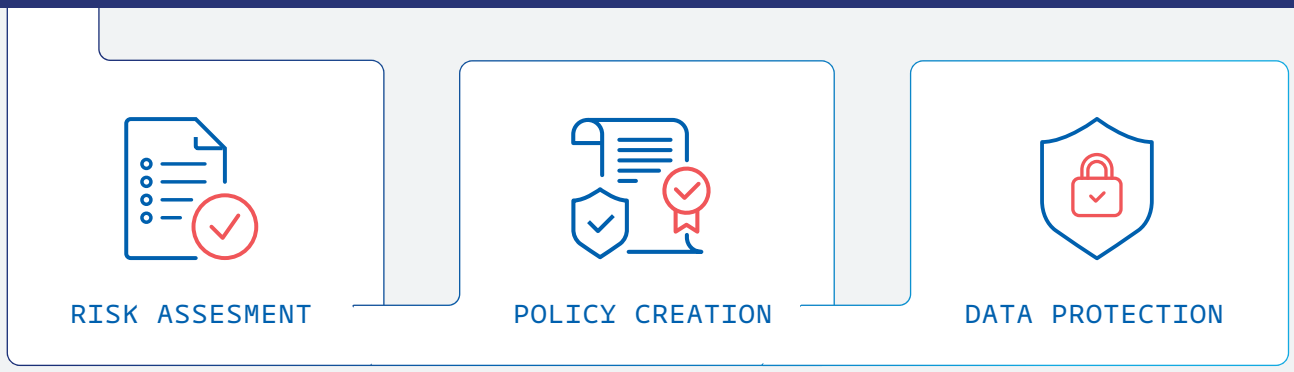
PK discovery PK encryption

Meeting NYCRR 500 Requirements with PK Discovery and PK Encryption

Becoming Familiar with 23 NYCRR 500

The State of New York adopted mandates and requirements for financial services institutions licensed or authorized by The New York State Department of Financial Services (DFS) to conduct business. 23 NYCRR 500 went into effect in March 2017, phasing in over a two-year period, with the final provisions having taken effect in March 2019.

The requirements take a broader approach to data security than any earlier US law, establishing minimum standards for a wide range of security activities, including risk assessment, policy creation, access control, data protection, and event reporting. Many of the law's provisions are similar to other recent data privacy regulations, including the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA), though the GDPR and the CCPA are more sweeping than 23 NYCRR500. Many entities covered by 23 NYCRR 500 are also within the jurisdictions of the GDPR and the CCPA. Some company efforts may simplify compliance with all three.



How Does 23 NYCRR 500 Affect Your 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. Costs of not implementing appropriate policies are considerable, both in financial terms and brand reputation damages. NY Banking law authorizes fees up to (a) $2,500 per day during which a violation continues (b) $15,000 per day in the event of any reckless or unsound practice or pattern of miscount, or (c) $75,000 per day in the event of a knowing and willful violation.

Covered entities will need to file an annual Certification of Compliance every April stating that they have met requirements in ensuring the continuous safeguarding of sensitive customer data, including:

- Established a formal cybersecurity program and document cybersecurity policies
- Conducted regular risk assessments
- Ensured the security of their applications
- Implemented data protection methods including encryption
- Used appropriate controls to limit access to sensitive information
- Notified the New York DFS within 72 hours in the event of a data breach or security incident

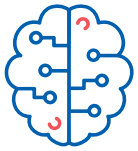
In addition, the law indirectly establishes rules for third party service providers that have access to covered entities' nonpublic information. Covered organizations are required to develop third party security policies that will effectively apply many 23 NYCRR 500 mandates to service providers who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

Integrated Discovery for Improved Protection

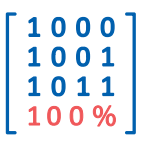
EXTENSIVE PLATFORM SUPPORT

SCALES TO ANY COMPANY SIZE

UNLIMITED SCANNING



MACHINE LEARNING



ELIMINATE FALSE NEGATIVES

How Do PK Discovery and PK Encryption Work Together to Help Meet 23 NYCRR 500 Requirements?

PK Discovery and PK Encryption combine intelligent data discovery, classification, and data protection to enable enterprise-wide control over sensitive data. Financial services organizations and their third party service providers can improve their data security and privacy protection while ensuring compliance with 23 NYCRR 500 and other government regulations and industry mandates.

23 NYCRR 500 Requirement	PK Discovery and PK Encryption
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. PK Discovery data discovery tools enable organizations to detect sensitive information on end user devices and in network storage locations. PK 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)	PK Encryption 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, PK Encryption is the only solution that facilitates true enterprise-wide encryption.
Application Security (Section 500.08)	PKWARE's software development kit for PK Discovery and PK Encryption 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, ensuring that proprietary applications comply with NYCRR 500 requirements.
Audit Trails And Activity Monitoring (Section 500.06 & 500.14)	PK Encryption web-based manager console facilitates complete administrative control over encrypted information. Access control lists determine who is authorized to decrypt protected information, while PK Encryption Data Security Intelligence tools provide full reporting on every encryption and decryption operation.
Third Party Security Policies (Section 500.11)	PK Encryption 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)	PK Discovery and PK Encryption take policy-based actions on files across the entire enterprise. By using PK Discovery's sensitive discovery and classification capabilities, organizations can define deletion criteria and automatically delete files according to data retention policies and any other files that are no longer needed.

The Broadest Support in the Market

Relational Databases (RDBMS) and Structured Data Store	• Amazon Aurora • Microsoft SQL Server • Green Plum • MySQL • IBM Db2	• IBM Db2 for z/OS • IBM Power Systems (AS/400) • Oracle • PostgreSQL • Sybase MariaDB
Data Warehouses	• Amazon Redshift • Google BigQuery	• IBM Netezza • Teradata
Big Data Hadoop Platforms	• Amazon Elastic MapReduce (EMR) • Cloudera • Google Cloud Dataproc	• Hortonworks • MapR • Microsoft Azure HDInsight
NoSQL Databases	• Cassandra	
Cloud Object Stores	• Amazon Simple Storage Service (s3) • Google Cloud Storage	• Microsoft Azure Blob Storage • Microsoft Azure Data Lake Storage
Inflight Data Transfers	• Via API Library	
On-Premises File Servers	• Linux	• Microsoft Windows
Endpoints	• Windows • macOS	• Ubuntu • CentOS
File Servers	• Windows Server • Ubuntu	• CentOS

BOOK A DEMO

Ready To See It Live? Contact Us!

pkware.com/demo

866-583-1795

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

Follow Us

/company/PKWARE

facebook.com/PKWARE

@PKWARE

NASSCOM ISO 27001 ISO 9001 Silver Microsoft Partner

PKWARE