New York State Cybersecurity Requirements of Financial Services Companies 23 NYCRR 500

What is the NYDFS Cybersecurity Law?

"The NYDFS Cybersecurity Regulation (23 NYCRR 500) is a new set of regulations from the NY Department of Financial Services (NYDFS) that places new cybersecurity requirements on all covered financial institutions. The rules were released on February 16th, 2017 after two rounds of feedback from industry and the public. These regulations acknowledge the ever-growing threat posed to financial systems by cybercriminals and are designed to ensure businesses effectively protect their customers' confidential information from cyber attacks. This includes conducting regular security risk assessments, keeping audit trails of asset use, providing defensive infrastructures, maintaining policies and procedures for cybersecurity, and creating an incident response plan.

Who does the NYDFS Cybersecurity Law Apply to?

- Credit Unions
- Health Insurers
- Investment Companies
- Licensed Lenders
- Life Insurance Companies
- Mortgage Brokers
- Savings and Loan Associations
- Private Brokers
- Offices of Foreign Banks
- Commercial Banks

What is Data Sanitization?

According to the Data Sanitization Consortium, "Data Sanitization is the process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable. A device that has been sanitized has no usable residual data, and even with the assistance of advanced forensic tools, the data will not ever be recovered. There are three methods to achieve data sanitization: physical destruction, cryptographic erasure, and data erasure."

Although data destruction and data sanitization have similarities in their approach, they are not the same. Data destruction does not include verification or certification of successful destruction beyond forensic recovery. This means that the chosen data destruction method has not been proven to remove data in totality, whether that target data is a single file or an entire drive.

Visit www.clarabyte.com to read our eBook on Data Sanitization Best Practices.

SPECIFICATION	DATA SANITIZATION SIMPLIFICATION
Section 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 operators 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.	Prove compliance by implementing and enforcing a data sanitization policy.

Clarabyte's data sanitization solutions help to protect sensitive data and guarantee compliance with NYDFS

Clarabyte's intuitive and flexible data erasure software allows highly-regulated organizations to easily automate their data sanitization processes to improve security, eliminate the risk of human error when processing devices, and to guarantee compliance with NYDFS. Clarabyte's proprietary algorithm offers data erasure for the entire spectrum of hard drives and solid-state drives, with verification of in successful erasure, and tamper-proof reporting. This unmatched level of control over data removal eliminates the risk that any data will ever be recovered without authorization so that devices may be securely reused, sold, or donated. No other data sanitization method is able to compare in risk elimination, scalability, or automation.

Click here to learn more about ClaraWipe Pro.

References:

https://www.mdsny.com/how-to-meet-dfs-23nycrr-500-in-five-steps/

https://www.datasanitization.org/