MorganFranklin Consulting A Vaco Company

Amendment to NYDFS Part 500

A Guide to the Amendments to the 23 NYCRR Part 500 Regulation

Amendments to 23 NYDFS Part 500

On November 1, 2023, the New York Department of Financial Services finalized amendments to their Cybersecurity Regulation 23 NYCRR Part 500, initially effective March 1, 2017.

MorganFranklin Cybersecurity consulting has reviewed the amendments and has summarized what we consider the more notable changes for our clients and other enterprises. Note that there is also a degree of interpretation and commentary that is included.

A comparative illustration of how the requirement sections of the content has been updated.

2017 NYDFS Part 500 - Sections	Amendment 2 - Sections
(02) Cybersecurity Program	(02) Cybersecurity Program
(03) Cybersecurity Policy	(03) Cybersecurity Policy
~~(04) Chief Information Security Officer~~	**(04) Cybersecurity Governance**
~~(05) Penetration Testing and Vulnerability Assessments~~	**(05) Vulnerability Management**
(06) Audit Trail	(06) Audit Trail
~~(07) Access Privileges~~	**(07) Access Privileges and Management**
(08) Application Security	(08) Application Security
(09) Risk Assessment	(09) Risk Assessment
(10) Cybersecurity Personnel and Intelligence	(10) Cybersecurity Personnel and Intelligence
(11) Third Party Service Provider Security Policy	(11) Third Party Service Provider Security Policy
(12) Multi-factor Authentication	(12) Multi-factor Authentication
~~(13) Limitations on Data Retention~~	**(13) Asset Management and Data Retention Requirements**
~~(14) Training and Monitoring~~	**(14) Monitoring and Training**
(15) Encryption of Nonpublic Information	(15) Encryption of Nonpublic Information
~~(16) Incident Response Plan~~	**(16) Incident Response and Business Continuity Management**
(17) Notices to Superintendent	(17) Notices to Superintendent
(18) Confidentiality	(18) Confidentiality
(19) Exemptions	(19) Exemptions
(20) Enforcement	(20) Enforcement
(21) Effective Date	(21) Effective Date
(22) Transitional Periods	(22) Transitional Periods

Summary of Notable Requirement Changes to NYDFS Part 500

Part 500 Section		DESCRIPTION SUMMARY
(07) Access Privileges and Management	500.07	Access Privileges and Management expectations are to mature towards a zero-trust approach.
	500.07 (a) (3)	The use of just-in-time (JIT) or fire-ID access for privileged accounts.
	500.07 (a) (4)	User access reviews no less than annually.
	500.07 (c) (1)	An access management system to manage all privileged accounts.
	500.07 (c) (2)	A system to block commonly used passwords on all accounts. An step change from common industry recommended requirements of password length, complexity, change frequency and reuse. Though possible through Microsoft AD services, Linux/Unix systems will be more challenged.
(08) Application Security	500.08 (b)	Secure application development processes and procedures reviewed, assessed an updated at least annually, from periodically.
(09) Risk Assessment	500.09 (a)	Annual, from periodic, risk assessment is required, or in the event of a material business or technology change to cyber risk.
(10) Cybersecurity Personnel and Intelligence		No notable changes
(11) Third Party Service Provider Security Policy		No notable changes

Summary of Notable Requirement Changes to NYDFS Part 500

Part 500 Section		DESCRIPTION SUMMARY
(02) Cybersecurity Program	500.02 (c)	Independent audit. The "independent audit" requirement will be new for most entities. Most audits tend to be limited to specific cybersecurity controls for platforms, i.e., SOC2 II, but this requirement is not only holistic, but likely more invasive for most entities as it seeks to audit the whole cybersecurity program.
	500.02 (e)	Program documentation is to made upon request to superintendent.
(03) Cybersecurity Policy	500.03	BOD must now approve cybersecurity policy annually and requires that program procedures be developed in support of the policy and cover 15 specific minimal areas.
(04) Cybersecurity Governance	500.04 (c)	Timely reporting by CISO to BOD of significant events or changes to the cybersecurity program.
	500.04 (d)	The BOD is assumed to demonstrate its commitment to understanding of its cybersecurity program and activities and the necessary funding to maintain it's effectiveness.
(05) Vulnerability Management	500.05 (a) (1)	Vulnerability management is more specified to include internal and external information systems boundary penetration testing.
	500.05 (a) (2)	Vulnerability scanning is more specified to include automated scans supplemented with manual reviews of unscanned systems.
(06) Audit Trail		No notable changes

Summary of Notable Requirement Changes to NYDFS Part 500

Part 500 Section		DESCRIPTION SUMMARY
(12) Multi-factor Authentication	500.12 (a)	MFA requirement changed from "may" be included to "shall be" and is to be utilized for anyone accessing its information systems for several newly specified areas;
	500.12 (a) (1)	remote access to information systems,
	500.12 (a) (2)	remote access to third-party systems with NPI,
	500.12 (a) (3)	privileged accounts, except for service accounts, and
	500.12 (b)	CISO is now required to annually approve equivalent or more secure compensating controls.
(13) Asset Management and Data Retention Requirements	500.13 (a)	Asset Management has been added to the data retention section and requires not only to have policies and procedures but specifies "key" asset information to be tracked including [risk] classification, [vendor EOL] support expiration date, recovery time objective and the frequency required to update and validate the asset inventory.
(14) Monitoring and Training	500.14 (a)	Monitoring requirements now include additional specifications to implement controls for protection from malicious code that also protects web traffic and email.
	500.14 (a) (3)	Cybersecurity awareness training for all personnel requirements are now at least annually and must include social engineering.
(15) Encryption of Nonpublic Information	500.15 (b)	Compensating controls for encryption requirements increase for the CISO to approve in writing and review at least annually.

Summary of Notable Requirement Changes to NYDFS Part 500

Part 500 Section		DESCRIPTION SUMMARY
(16) Incident Response and Business Continuity Management	500.16 (a) (1) (viii)	The post incident response processes highlight both a thorough and a leading practice insistence for entities. For example, root cause analysis, which tends to be more formalized in IT organizations than in cybersecurity, is a new requirement. The addition clearly is intended to increase organizational maturity.
	500.16 (a) (2)	The BCP and DR requirements added provide a proscriptive program for entities, from what the scope of the plans are to include (systems, material services, personnel, assets and NPI) as well as specifications to be included in the plans, such as documents, data, facilities. All the plan requirements you would expect to see in a thorough BCP and DR program.
(17) Notices to Superintendent	500.17 (a) (1)	The 72 notification to the superintendent remains, but now includes occurrences with affiliates and third-party service providers. Additionally in an apparent effort to be more consistent with industry / ITSM nomenclature, notification of a "cybersecurity event" is replaced with "cybersecurity incident". Cybersecurity incident means a cybersecurity event that has occurred at the covered entity, its affiliates, or a third-party service provider that: (1) impacts the covered entity; (2) a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity; or (3) results in the deployment of ransomware within a material part of the covered entity's information systems.

Summary of Notable Requirement Changes to NYDFS Part 500

Part 500 Section		DESCRIPTION SUMMARY
(16) Incident Response and Business Continuity Management	500.17 (a) (2)	A new requirement for continuous updates on incidents. It best illustrates the agencies desire to be more informed in understanding incidents at a more detailed level. This may be interpreted as an active additional governing body unto itself versus oversight role on an entity's resulting actions.
	500.17 (b) (1) (i) (b)	Annual certification has been added and includes attesting to material compliance with the requirements and supporting sufficient documentation to "accurately" support such claim.
(17) Notices to Superintendent	500.17 (b) (2)	Certification to the Superintendent is to be provided by both the CISO and the CEO.
	500.17 (b) (3)	Retention of annual attestation and supporting documentation of compliance is for five years.
	500.17 (c)	Notify Superintendent of extortion payment with two notable deliverable dates.
	500.17 (c) (1)	Notify of extortion payment within 24 hours.
	500.17 (c) (2)	Within 30 days; - provide written description of reasons why payment was required, - what alternatives were considered, - diligence performed to find alternatives, and - diligence to support compliance with rules and regulations including those of the Office of Foreign Assets Control.

Summary of Notable Requirement Changes to NYDFS Part 500

Part 500 Section		DESCRIPTION SUMMARY
(18) Confidentiality		No notable changes
(19) Exemptions		No notable changes
(20) Enforcement		No notable changes
(21) Effective Date	500.21 (b)	Amendment 2 effective November 1, 2023.
(22) Transitional Periods		Refer to the Transition Period timeline on the follow page.
(18) Confidentiality		No notable changes
(19) Exemptions		No notable changes

Timeline for Navigating Transition Periods

Navigating the multitude of changes introduced by the expanded NYDFS regulations might seem like a daunting task for companies. However, a well-structured timeline can serve as a practical guide to implementing these adjustments seamlessly.