Due diligence checklist: NYDFS Part 500

23 NYCRR Part 500, Cybersecurity Requirements for Financial Services Companies. NYDFS, the United States.

Regime	NYDFS Part 500
Regulator	NYDFS
Country	the United States
Regulator's page	https://www.dfs.ny.gov/industry_guidance/cybersecurity
Prepared	9 November 2026
Current version	https://www.vederca.com/market-scan/due-diligence/us-nydfs

What it is

A written policy for third-party providers: due diligence, minimum controls and periodic assessment.

Who it applies to

Applies to every financial institution in the United States.

What to ask a vendor, and the evidence to request

#	Ask the vendor for	Evidence to request	Received
1	Multi-factor authentication, encryption and access controls that meet Part 500	A description of the security controls, the most recent control testing or penetration test summary, and the policies for vulnerability, change and access management.	
2	Notice of cybersecurity events in time for the institution's 72-hour report to the Department	The incident notification clause and procedure: what counts as an incident, who is told, within what time, and a record of a past notification if one exists.	

In every case

- A named contact at the vendor responsible for this regime, and how the vendor tracks changes to it.
- Which named customers the vendor already serves under this regime, as references you may call.

This checklist is a starting point for a procurement team, not legal advice. Read it with the regulator's own page, your institution's policies and your legal and risk teams; the regime may have changed since the date on this document.