How does Cyber Crucible support New York DFS Part 500 cybersecurity requirements?

Short answer: For a financial institution covered by New York DFS Part 500 (23 NYCRR 500), Cyber Crucible supports several required controls — multi-factor authentication, encryption, access controls, and incident response — while reducing third-party risk because it never collects the nonpublic information the rule protects. Cyber Crucible is a third-party service provider under the rule, not a covered entity itself.

Controls it supports

- **Access controls and MFA** for the management dashboard, backed by strong authentication.
- **Encryption** of data in transit and at rest.
- **Incident response** under a documented breach-response process, with a committed notification timeframe available by contract — supporting the covered entity's 72-hour DFS notification obligation.
- **Third-party risk reduction** through data minimization: no nonpublic information is collected.

The honest boundary

Part 500's obligations — CISO designation, risk assessment, the annual certification — rest with the covered entity. Cyber Crucible supplies control evidence for the entity's third-party service provider policy (500.11). It is not a covered entity and holds no Part 500 "certification." Evidence is provided under NDA.

Revision #2
Created 2026-07-23 15:18:35 UTC by Dennis Underwood
Updated 2026-07-23 18:20:03 UTC by Dennis Underwood