Comment Cyber Crucible soutient-il les exigences de cybersécurité de la New York DFS Part 500 ?

Réponse courte : Pour une institution financière soumise à la New York DFS Part 500 (23 NYCRR 500), Cyber Crucible soutient plusieurs contrôles requis — authentification multifacteur, chiffrement, contrôles d'accès et réponse aux incidents — tout en réduisant le risque tiers, car il ne collecte jamais les informations non publiques que la réglementation protège. Cyber Crucible est un prestataire de services tiers au sens de la réglementation, et non une entité couverte elle-même.

Contrôles pris en charge

- **Contrôles d'accès et MFA** pour le tableau de bord de gestion, appuyés par une authentification forte.
- **Chiffrement** des données en transit et au repos.
- **Réponse aux incidents** dans le cadre d'un processus documenté de réponse aux violations, avec un délai de notification garanti disponible contractuellement — soutenant l'obligation de notification de 72 heures de la DFS pour l'entité couverte.
- **Réduction du risque tiers** grâce à la minimisation des données : aucune information non publique n'est collectée.

La limite en toute honnêteté

Les obligations de la Part 500 — désignation d'un CISO, évaluation des risques, certification annuelle — relèvent de la responsabilité de l'entité couverte. Cyber Crucible fournit des éléments de preuve de contrôle pour la politique de prestataires de services tiers de l'entité (500.11). Il ne s'agit pas d'une entité couverte et ne détient aucune « certification » Part 500. Les éléments de preuve sont fournis sous accord de confidentialité (NDA).

Revision #1
Created 2026-07-24 07:16:07 UTC by Dennis Underwood
Updated 2026-07-24 07:16:07 UTC by Dennis Underwood