Harborview Insurance Agency

NYDFS annual assessment - 2026

Generated November 18, 2026 15:30 UTC

Buffalo Sentinel
Compliance Platform

Status: Completed November 18, 2026 by Dana Whitfield
Started: November 4, 2026 by Dana Whitfield
Evidence as of: November 18, 2026
Classification: Covered entity (not Class A, no exemption)
Applicable requirements: 42 (36 compliant, 6 gaps, 0 open)
Not applicable or exempt: 12 (7 by classification, 5 answered "does not apply")
Questions answered: 27 of 27

Scope

Covered entity without an exemption: every requirement applies except the Class A items.

47 requirement(s) apply: 27 need your answer, the rest are decided by records already in Buffalo Sentinel or need a record on the linked page.

Results by area

Area	Compliant	Gaps	Open	Exempt / N/A
Governance & program	8	0	0	0 / 2
Policies	2	0	0	0 / 2
Access & identity	6	2	0	0 / 6
Risk assessment	4	2	0	0 / 0
Vendors	2	0	0	0 / 0
Data & assets	5	0	0	0 / 2
Training	0	1	0	0 / 0
Incident response & continuity	6	1	0	0 / 0
Notices & filing	3	0	0	0 / 0

Gaps to fix (6)

Requirement	Status	Why	How to fix
500.7(a)(5) Disable or secure remote-control protocols Access & identity	Not compliant	Answered not in place on Nov 6, 2026 by Dana Whitfield. *Remediation plan: Not fully in place: Remote Desktop is enabled without Network Level Authentication on one computer. Northline IT will turn on NLA and remove unused RDP access.*	Fix the gap, then answer again in the assessment /compliance/policies
500.12(a) MFA for any individual accessing any information system Access & identity	Partially compliant	22 of 24 active identity-provider accounts enrolled in MFA. Microsoft 365: 22 of 24 enrolled	Connect Microsoft 365, Okta or Duo to measure MFA coverage /mfa
500.5(a)(1) Penetration testing at least annually Risk assessment	Not compliant	Penetration test completed last on Oct 14, 2025; overdue since Oct 14, 2026	Record the penetration test /compliance/security-assessments

500.5(c) Timely remediation of vulnerabilities Risk assessment	Partially compliant	23 of 25 devices (92%) have no Critical or Security update missing for more than 14 days (agent Windows Update scans). 2 device(s) have Critical or Security updates missing past the grace period.	Track remediation of open findings and missing patches /compliance/security-assessments
500.14(a)(3) Annual cybersecurity awareness training including social engineering Training	Partially compliant	21 of 24 active identity-provider accounts (87%) completed awareness training with social engineering content in the last 12 months (threshold: 95% of personnel in scope within 12 months). 3 people have a mapped training assignment past due.	Assign and complete the annual awareness training /training
500.16(d)(1) Annual testing of the incident response and BCDR plans Incident response & continuity	Partially compliant	Incident response plan tested Mar 12, 2026; BCDR plan test never recorded	Record the annual plan test /compliance/continuity-testing

Answers given in this assessment (27)

Requirement	Answer	Statement	Answered by
500.2(a) Maintain a cybersecurity program	In place	Harborview maintains a written cybersecurity program based on the 2026 risk assessment. Northline IT runs day-to-day operations under the managed services agreement. Documentation: IT Security Program v4 (SharePoint > Compliance > NYDFS)	Dana Whitfield November 4, 2026, valid until November 4, 2027
500.2(b) Core cybersecurity functions	In place	The program identifies risks, protects systems and data, detects and responds to events, recovers, and meets our reporting obligations. Each function is mapped to a control owner. Documentation: IT Security Program v4, section 2	Dana Whitfield November 4, 2026, valid until November 4, 2027
500.2(d) Adopting an affiliate's cybersecurity program	Does not apply	Harborview maintains its own program and does not adopt an affiliate's.	Dana Whitfield November 4, 2026, valid until November 4, 2027
500.2(e) Program documentation available to the superintendent on request	In place	Program documents, policies, test results and this assessment are kept in the Compliance library and can be produced on request. Documentation: SharePoint > Compliance > NYDFS	Dana Whitfield November 4, 2026, valid until November 4, 2027
500.4(c) Timely reporting of material cybersecurity issues	In place	The vCISO reports material issues to the President and the board chair within one business day; three escalations were made this year. Documentation: CISO escalation log	Dana Whitfield November 5, 2026, valid until November 5, 2027
500.10 Cybersecurity Personnel and Intelligence	In place	Cybersecurity functions are performed by Northline IT under contract, overseen by the designated CISO. Staff receive threat advisories monthly. Documentation: Managed services agreement, schedule B	Dana Whitfield November 5, 2026, valid until November 5, 2027
500.7(b) Written password policy	In place	Password policy requires 14 or more characters and MFA; passwords are checked against breached password lists in Microsoft 365. Documentation: Access Control Policy v3, section 4	Dana Whitfield November 5, 2026, valid until November 5, 2027

500.8(a) Secure development and external application security procedures	Does not apply	Harborview does not develop applications in house; all applications are vendor products.	Dana Whitfield November 5, 2026, valid until November 5, 2027
500.8(b) Annual CISO review of application security procedures	Does not apply	No in-house development (see 500.8(a)).	Dana Whitfield November 5, 2026, valid until November 5, 2027
500.7(a)(1) Limit user access to what the job requires	In place	Access is granted by role through Microsoft 365 groups; the agency management system has separate producer, CSR and accounting roles. Documentation: Access Control Policy v3, role matrix	Dana Whitfield November 6, 2026, valid until November 6, 2027
500.7(a)(2) Limit privileged accounts and their functions	In place	Two administrator accounts exist (owner and Northline IT break-glass), both with MFA and no mailbox. Documentation: Privileged account register	Dana Whitfield November 6, 2026, valid until November 6, 2027
500.7(a)(3) Use privileged accounts only when required	In place	Administrators use separate admin accounts only for administrative tasks. Documentation: Access Control Policy v3, section 6	Dana Whitfield November 6, 2026, valid until November 6, 2027
500.7(a)(5) Disable or secure remote-control protocols	Not in place (gap)	Not fully in place: Remote Desktop is enabled without Network Level Authentication on one computer. Northline IT will turn on NLA and remove unused RDP access. Documentation: Remote access inventory, November 2026	Dana Whitfield November 6, 2026, valid until November 6, 2027
500.7(a)(6) Promptly terminate access after departures	In place	Departing staff are disabled in Microsoft 365 and the agency system on their last day using the offboarding checklist. Documentation: Offboarding checklist (HR)	Dana Whitfield November 6, 2026, valid until November 6, 2027
500.12(b) CISO-approved compensating controls, reviewed at least annually	Does not apply	No compensating controls are used for MFA; MFA is required for all users.	Dana Whitfield November 6, 2026, valid until November 6, 2027
500.14(a)(1) Monitor authorized user activity	In place	Sign-in activity is monitored through Microsoft 365 alerts and the endpoint agent; alerts go to Northline IT. Documentation: Monitoring runbook	Dana Whitfield November 7, 2026, valid until November 7, 2027
500.5(b) Monitoring for new security vulnerabilities	In place	Northline IT subscribes to CISA KEV and vendor advisories and reviews new vulnerabilities weekly. Documentation: Vulnerability management procedure	Dana Whitfield November 7, 2026, valid until November 7, 2027
500.11(b) Due diligence and contractual protection guidelines	In place	Vendor contracts require MFA, encryption and breach notice within 72 hours; terms are tracked per vendor. Documentation: Vendor Management Policy v2	Dana Whitfield November 8, 2026, valid until November 8, 2027
500.6 Audit Trail	In place	Audit trails are kept for Microsoft 365 (unified audit log, 180 days) and the agency system; endpoint audit policy is applied by GPO. Documentation: Logging standard	Dana Whitfield November 8, 2026, valid until November 8, 2027
500.13(b) Secure disposal of nonpublic information	In place	Paper files are shredded by a bonded vendor; retired drives are wiped and certificates kept. Documentation: Data Retention and Disposal Policy	Dana Whitfield November 8, 2026, valid until November 8, 2027
500.14(a)(2) Malicious	In place	Microsoft Defender runs on every computer;	Dana Whitfield

code protection, including web and email filtering		Microsoft 365 web and email filtering is on. Documentation: Endpoint standard	November 8, 2026, valid until November 8, 2027
500.15(a) Written encryption policy for data in transit and at rest	In place	Encryption policy requires TLS in transit and BitLocker at rest; exceptions go to the CISO. Documentation: Encryption Policy v2	Dana Whitfield November 9, 2026, valid until November 9, 2027
500.15(b) Compensating controls where encryption at rest is infeasible	Does not apply	Encryption at rest is feasible everywhere: BitLocker is required on every computer and the file server, so no compensating controls are used.	Dana Whitfield November 9, 2026, valid until November 9, 2027
500.16(b) Plans distributed and accessible	In place	Plans are in the Compliance library and printed in the office binder; key contacts carry the call tree. Documentation: Incident Response Plan v3	Dana Whitfield November 9, 2026, valid until November 9, 2027
500.16(c) Training on the plans	In place	Staff were trained on the incident response plan during the March tabletop exercise. Documentation: Tabletop exercise report, March 2026	Dana Whitfield November 9, 2026, valid until November 9, 2027
500.17(a) Notice of cybersecurity incident within 72 hours	In place	No reportable cybersecurity incidents (incidents requiring notice to the superintendent under 23 NYCRR 500.17(a)) occurred during Nov 11, 2025 to Nov 10, 2026. Documentation: Incident Response Plan v3, section 7	Dana Whitfield November 10, 2026, valid until November 10, 2027
500.17(c) Notice and explanation of extortion payment	In place	No extortion payments were made in connection with a cybersecurity event during Nov 11, 2025 to Nov 10, 2026 (23 NYCRR 500.17(c)). Documentation: Incident Response Plan v3, section 8	Dana Whitfield November 10, 2026, valid until November 10, 2027

April 15 annual notice of compliance (500.17(b))

The annual notice of compliance for 2026 is due Apr 15, 2027 (500.17(b)). The Annual Certification page checks the same evidence when it is signed: each gap listed here blocks a Certification of Material Compliance until it is fixed or a signer records why the requirement was nonetheless materially complied with. Otherwise, list it in an Acknowledgment of Noncompliance with a remediation timeline.

About this document

Status as of Nov 18, 2026 from the company's records in Buffalo Sentinel and the answers given in this assessment. It helps track compliance and is not a legal determination or a filing with DFS.

Each answer is an attestation, valid for 12 months, and counts only where no platform record decides the requirement.