Harborview Insurance Agency

CISO annual written report to the senior governing body - 2026

Generated November 18, 2026 15:30 UTC

Chief Information Security Officer: Marcus Ortega

Period covered: January 1, 2026 to December 31, 2026

Report date: -

Status: Draft (not approved by the CISO)

NYDFS requirement status (platform records): 36 of 42 applicable requirements compliant, 4 partial, 2 not compliant, 0 need evidence

Required contents (500.4(b)(1)-(6), to the extent applicable)

Addressed	500.4(b)(1) Confidentiality of nonpublic information and the integrity and security of information systems
Addressed	500.4(b)(2) Cybersecurity policies and procedures
Addressed	500.4(b)(3) Material cybersecurity risks
Addressed	500.4(b)(4) Overall effectiveness of the cybersecurity program
Addressed	500.4(b)(5) Material cybersecurity events during the period
Addressed	500.4(b)(6) Plans for remediating material inadequacies

Executive summary

This report covers Jan 1, 2026 to Dec 31, 2026 for Harborview Insurance Agency. 36 of 42 applicable NYDFS requirements are shown compliant from platform records; 6 have gaps and 0 need evidence. No reportable cybersecurity incidents were recorded. 2 critical or high risk(s) remain open.

500.4(b)(1) Confidentiality of nonpublic information and the integrity and security of information systems

Status of the controls that protect nonpublic information and the integrity and security of the information systems, from the platform's records as of Nov 18, 2026:
- 500.7(a)(1) Limit user access to what the job requires: Compliant. Attested compliant on Nov 6, 2026 by Dana Whitfield (valid until Nov 6, 2027).
- 500.7(a)(2) Limit privileged accounts and their functions: Compliant. Attested compliant on Nov 6, 2026 by Dana Whitfield (valid until Nov 6, 2027).
- 500.7(a)(4) Review user access privileges at least annually: Compliant. User access review completed on Dec 12, 2025; next due Dec 12, 2026 (within 30 days).
- 500.7(a)(6) Promptly terminate access after departures: Compliant. Attested compliant on Nov 6, 2026 by Dana Whitfield (valid until Nov 6, 2027).
- 500.12(a) MFA for any individual accessing any information system: Partially compliant. 22 of 24 active identity-provider accounts enrolled in MFA.
  Supporting: RDP Network Level Authentication (1 of 2 devices).
- 500.13(a) Asset inventory: Compliant. All 38 assets record owner, location, classification, support expiration and RTO, validated within 180 days.
- 500.14(a)(2) Malicious code protection, including web and email filtering: Compliant. Attested compliant on Nov 8, 2026 by Dana Whitfield (valid until Nov 8, 2027).
- 500.15(a) Written encryption policy for data in transit and at rest: Compliant. Attested compliant on Nov 9, 2026 by Dana Whitfield (valid until Nov 9, 2027).
  Supporting: BitLocker on system drives (24 of 25 devices).
- 500.5(c) Timely remediation of vulnerabilities: Partially compliant. 23 of 25 devices (92%) have no Critical or Security update missing for more than 14 days (agent Windows Update scans).
- 500.6 Audit Trail: Compliant. Attested compliant on Nov 8, 2026 by Dana Whitfield (valid until Nov 8, 2027).
- 500.16(e) Backups maintained and protected: Compliant. All 2 active backup(s) protected from alteration or destruction (immutable or isolated).

500.4(b)(2) Cybersecurity policies and procedures

9 cybersecurity policies are in force; 9 were approved by a senior officer or the senior governing body in the last 12 months.

- 500.3 Cybersecurity Policy: Compliant. All 15 applicable 500.3 areas are addressed by policies approved by a senior officer or the senior governing body in the last 12 months.

500.4(b)(3) Material cybersecurity risks

- 500.9(a) Risk assessment, updated at least annually: Compliant. Risk assessment "2026 Annual Cyber Risk Assessment" approved Mar 26, 2026 covers the business operations, nonpublic information and information systems; next update due Mar 26, 2027.
Latest risk assessment: 2026 Annual Cyber Risk Assessment (Mar 26, 2026), overall risk level Moderate.
Open risks in the register: 11 (0 critical, 2 high, 5 medium, 4 low); 1 past their treatment due date.
Material risks (critical and high):
- R-03 Business email compromise leading to fraudulent premium or claim payments (high): treatment Mitigate: payment call-back procedure, Email Protection, MFA for all users, owner Dana Whitfield, due Dec 15, 2026.
- R-07 Out-of-support scanner workstation (Windows 10) on the office network (high): treatment Mitigate: replace the workstation, owner Chris Albright, due Nov 27, 2026.

500.4(b)(4) Overall effectiveness of the cybersecurity program

Classification: Covered entity (not Class A, no exemption). Of 42 applicable requirements, 36 are compliant, 4 partially compliant, 2 not compliant and 0 still need evidence (90% weighted). 20 are evidenced by platform records and 22 by attestation.
Sections not yet shown compliant:
- 500.5 Vulnerability Management: Not compliant. 2 of 4 applicable subsection(s) compliant; 1 partially compliant; 1 not compliant.
- 500.7 Access Privileges and Management: Not compliant. 6 of 7 applicable subsection(s) compliant; 1 not compliant.
- 500.12 Multi-Factor Authentication: Partially compliant. 0 of 1 applicable subsection(s) compliant; 1 partially compliant.
- 500.14 Monitoring and Training: Partially compliant. 2 of 3 applicable subsection(s) compliant; 1 partially compliant.
- 500.16 Incident Response and Business Continuity Management: Partially compliant. 6 of 7 applicable subsection(s) compliant; 1 partially compliant.
These statuses come from the records in Buffalo Sentinel; they help track compliance and are not a legal determination.

500.4(b)(5) Material cybersecurity events during the period

No reportable cybersecurity incidents (500.17(a)) were recorded for Jan 1, 2026 to Dec 31, 2026.

500.4(b)(6) Plans for remediating material inadequacies

Open security assessment findings: 2 (0 critical or high).
Risk treatments for 2 critical or high risks are listed under material cyber risks.
Requirements to remediate (not compliant or partially compliant):
- 500.5(a)(1) Penetration testing at least annually: Not compliant. Penetration test completed last on Oct 14, 2025; overdue since Oct 14, 2026.
- 500.5(c) Timely remediation of vulnerabilities: Partially compliant. 23 of 25 devices (92%) have no Critical or Security update missing for more than 14 days (agent Windows Update scans).
- 500.7(a)(5) Disable or secure remote-control protocols: Not compliant. Attested not compliant on Nov 6, 2026 by Dana Whitfield (valid until Nov 6, 2027).
- 500.12(a) MFA for any individual accessing any information system: Partially compliant. 22 of 24 active identity-provider accounts enrolled in MFA.
- 500.14(a)(3) Annual cybersecurity awareness training including social engineering: 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).
- 500.16(d)(1) Annual testing of the incident response and BCDR plans: Partially compliant. Incident response plan tested Mar 12, 2026; BCDR plan test never recorded.

Compensating controls approved by the CISO (500.12(b), 500.15(b), 500.7(c)(2), 500.14(b))

No compensating controls are recorded in the register.

Harborview Insurance Agency

CISO annual written report to the senior governing body - 2026

Generated November 18, 2026 15:30 UTC

Approval and presentation

Not yet approved by the CISO.

Not yet presented to the senior governing body.

About this document. Sections were drafted from the organization's records in Buffalo Sentinel and edited by the CISO. Requirement statuses help track compliance and are not a legal determination. Keep this report with the records supporting the annual notice of compliance (500.17(b)).