IT & Security Status

Harborview Insurance Agency: October 2026 (October 1, 2026 to October 31, 2026)
Prepared by Northline IT on November 2, 2026

Dana, here is the October report for Harborview. Page one is the short version: what is in good shape, what needs attention and who does what next. The details and the technical appendix behind it follow. Call the help desk with any question.

Overall: Action needed

5 items need action soon and 13 more items should be looked at; 5 checks passed.

What's good

+ Antivirus or endpoint protection is running on every checked computer.
+ The firewall is on for every checked computer.
+ Every checked backup succeeded in the last 7 days.
+ A restore test succeeded in the last 12 months.

And 1 more check passed (see the details).

Needs attention

1. **1 vulnerability on your computers is known to be used in real attacks** [Urgent]
   Why it matters: Attackers are actively using these weaknesses right now.
   What to do: Update or remove the affected software first (listed in the appendix).
2. **2 of 25 computers are missing security updates older than 14 days** [High]
   Why it matters: Missing updates are one of the most common ways attackers get in.
   What to do: Install the pending updates and restart; find out why automatic updates are not finishing on these computers.
3. **1 high-severity security alert is open** [High]
   Why it matters: High alerts point to risky activity such as repeated failed sign-ins or protection being turned off.
   What to do: Review them this week and resolve or escalate each one.
4. **2 of 24 people sign in without MFA** [High]
   Why it matters: Without MFA, a stolen or guessed password is all it takes to get into their email.
   What to do: Turn on MFA for every account (security defaults, Conditional Access or a 2-Step Verification policy).

And 14 more items in the details.

What changed since last period

Compared with September 1 to September 30, 2026:

Worse	Open tickets: 6, up from 4
Better	Computers not checking in: 1, down from 2
Better	Computers without disk encryption: 1, down from 2

And 5 more in the details.

Next steps

Who	What to do
Northline IT (IT provider)	Update or remove the affected software first (listed in the appendix).
Northline IT (IT provider)	Install the pending updates and restart; find out why automatic updates are not finishing on these computers.
Northline IT (IT provider)	Review them this week and resolve or escalate each one.
Dana Whitfield	Finish "Vendor review: Coastline Payroll Services". Past due since Oct 28, 2026.

Details by area

Each area shows whether it could be checked and what was found. Areas that are not connected are never shown as good.

All changes from September 1 to September 30, 2026

Worse	Open tickets: 6, up from 4
Better	Computers not checking in: 1, down from 2
Better	Computers without disk encryption: 1, down from 2
Better	Computers missing security updates: 2, down from 5
Better	Open critical and high alerts: 1, down from 3
Better	Tickets past their due date: 1, down from 2
Better	Tickets that missed a target: 0, down from 3
Better	People using MFA: 92%, up from 79%

Computers and devices

Needs attention

5 device problems were found; 25 of 26 computers checked in.

Computers	26
Checked in within 30 days	25
Not checked in for 30+ days	1
Unsupported operating system	1 of 25
No antivirus or endpoint protection	0 of 25
Disk not encrypted	1 of 25
Firewall off	0 of 25
Remote access paths open	4
Remote support tools nobody approved	0
Remote access paths without MFA evidence	1

[Medium] 1 computer has not checked in for over 30 days. Confirm each one is still in use: restart the agent, or retire the computer in the portal.

[Medium] 1 computer runs an operating system that no longer gets security updates. Upgrade or replace these computers (listed in the appendix).

[Medium] 1 remote access path has no MFA evidence. Turn on MFA for these paths, record the Duo application that protects them, or confirm on the Remote access page how each one enforces it.

[Medium] Remote Desktop is on without Network Level Authentication on 1 computer. Turn on "Require Network Level Authentication" for Remote Desktop, or turn Remote Desktop off where nobody needs it.

[Low] 1 computer is not encrypted. Turn on BitLocker (Windows) or disk encryption (Linux) on these computers.

Security updates

Action needed

23 of 25 scanned computers are up to date.

Computers scanned	25
Up to date	23
Missing security updates older than 14 days	2
Missing Critical updates older than 7 days	2

[High] 2 of 25 computers are missing security updates older than 14 days. Install the pending updates and restart; find out why automatic updates are not finishing on these computers.

Security alerts and incidents

Action needed

23 alerts were raised and 21 resolved during the period. No security incident was recorded.

Alerts raised this period	23
Alerts resolved this period	21
Open critical	0
Open high	1
Open medium and low	3
Incidents recorded this period	0
Incidents closed this period	1
Incidents still open	0

[High] 1 high-severity security alert is open. Review them this week and resolve or escalate each one.

Tickets and requests

Needs attention

37 tickets were opened and 35 closed during the period; 6 are open now.

Opened this period	37
Closed this period	35
Open now	6
Past their due date	1
Missed a response or resolution target this period	0

[Medium] 1 open ticket is past the due date. Review the overdue tickets (listed in the appendix) and update, reassign or close them.

People: MFA, training and phishing

Action needed

MFA: 22 of 24 people. Training: 21 of 24 people current. Phishing test: 8% clicked.

People using MFA	22 of 24 (92%)
Administrators using MFA	2 of 2
Security training in the last 12 months	21 of 24 (88%)
Phishing test this period	24 sent, 2 clicked, 1 entered a password, 9 reported

[High] 2 of 24 people sign in without MFA. Turn on MFA for every account (security defaults, Conditional Access or a 2-Step Verification policy).

[Medium] 2 of 24 people clicked the test phishing email (8%) and 1 entered a password. Give the people who clicked a short refresher course, then test again.

[Medium] 3 of 24 people have not completed security training in the last 12 months. Assign the annual security awareness course and follow up with those who have not finished.

Backups

Good

Every checked backup succeeded in the last 7 days.

Backups with a success in the last 7 days	2 of 2
Restore test in the last 12 months	yes

Buffalo Sentinel Ark is not linked: backups are checked from the backup register and the agent's backup detection.

Email security

Needs attention

8,930 messages checked, 44 flagged. Email authentication is incomplete. A domain registration expires soon.

Mailboxes protected	24
Messages checked this period	8,930
Flagged suspicious	41
Flagged likely fraud	3
Domains with SPF, DKIM and DMARC	2 of 3
Domain registrations checked	3 of 3
Domains with DNS changes this period	1

[Medium] Email authentication (SPF, DKIM, DMARC) is incomplete for 1 domain. Publish SPF, DKIM and DMARC records for these domains.

[Medium] The domain harborview-insure-example.com expires in 23 days (November 25, 2026). Renew the domain with the registrar and turn on auto-renew.

[Low] DNS records changed for 1 domain: harborview-example.com. Confirm on the Domains page that each change was made on purpose.

Firewall and network

Needs attention

No urgent firewall findings; 1 setting needs attention.

Firewall consoles online	1 of 1
Sites checked	1 of 1
Open findings: critical	0
Open findings: high	0
Open findings: medium and low	1
Checks that could not run	0
Settings changes this period	0
Network devices (offline)	11 (0)
Last checked	November 2, 2026

[Medium] 1 firewall or Wi-Fi setting needs attention. Review the firewall findings in the appendix and plan the changes.

Vulnerabilities

Action needed

1 critical and 3 high vulnerabilities are open on 7 computers. 1 of them has been open for more than 30 days.

Critical	1
High	3
Medium and low	41
Known to be used in real attacks	1
Critical or high open more than 30 days	1
Computers affected	7

[Urgent] 1 vulnerability on your computers is known to be used in real attacks. Update or remove the affected software first (listed in the appendix).

[High] 1 critical vulnerability is open. Apply the vendor updates for the software listed in the appendix.

Compliance

For information

Enrolled in NYDFS Cybersecurity Regulation (23 NYCRR 500).

NYDFS Cybersecurity Regulation (23 NYCRR 500)	90% of applicable requirements met

A snapshot only: the compliance report in the portal (Reports) has the requirement detail.

Outstanding actions

Needs attention

7 action items are open; 1 past due.

Open action items	7
Past due	1
Without an owner	0

[Medium] 1 action item is past the due date. Finish them or set a realistic new date.

Technical appendix

For the IT team: the devices, vulnerabilities, alerts, tickets, actions and firewall findings behind page one.

A. Devices with problems

Active computers with at least one problem. A computer that has not checked in for 30 days is listed without other checks.

Computer	Operating system	Last check-in	Problems
HV-SCAN-01	Microsoft Windows 10 Pro	Nov 2, 2026	Windows 10: support ended 2025-10-14; 5 security updates overdue (2 Critical)
HV-AGENT-04	Microsoft Windows 11 Pro	Nov 2, 2026	3 security updates overdue (1 Critical)
HV-AGENT-06	Microsoft Windows 11 Pro	Nov 2, 2026	BitLocker is off
HV-LAPTOP-02	Microsoft Windows 11 Pro	not in 30 days	Not checked in for 30+ days

B. Top vulnerabilities

Open critical, high and known-exploited vulnerabilities on active computers, most urgent first (up to 15).

CVE	Severity	CVSS	Exploited	Software	Computers
CVE-2026-90311	critical	9.8	Yes	Windows 10 cumulative update (October 2026)	1: HV-SCAN-01
CVE-2026-90944	high	8.8	No	Google Chrome 129	2: HV-AGENT-04, HV-LAPTOP-03
CVE-2026-90807	high	7.8	No	7-Zip 22.01	1: HV-SCAN-01
CVE-2026-90530	high	7.5	No	Adobe Acrobat Reader 24.002	3: HV-CLAIMS-01, HV-CLAIMS-02, HV-CLAIMS-03

C. Open security alerts and incidents

Unresolved alerts (most severe first, up to 50) and open incidents.

Severity	Alert	Computer	Source	Last seen
high	Repeated failed sign-ins to a local administrator account (14 times)	HV-CLAIMS-02	Agent	Oct 31, 2026
medium	Microsoft Defender real-time protection was turned off and back on	HV-AGENT-06	Agent	Oct 24, 2026
medium	New inbox forwarding rule to an external address		SIEM	Oct 27, 2026
low	USB storage device connected (2 times)	HV-ACCT-01	Agent	Oct 29, 2026

D. Overdue and missed-target tickets

Open tickets past their due date and tickets that missed a response or resolution target.

Ticket	Subject	Priority	Status	Due	Assigned to	Problem
T-2214	Scanner on HV-SCAN-01 stops sending to the shared folder	Normal	Waiting on vendor	Oct 29, 2026	Chris Albright	Past due date (Help desk)

E. Outstanding actions

Open project tasks, compliance gaps and risk treatment actions, overdue first (up to 100).

Type	Item	Owner	Due	Overdue
Risk treatment	Vendor review: Coastline Payroll Services	Dana Whitfield	Oct 28, 2026	Yes
Compliance gap	Schedule and record the 2026 penetration test (500.5(a)(1))	Dana Whitfield	Nov 20, 2026	
Project task	Replace HV-SCAN-01 (Windows 10 is out of support)	Chris Albright	Nov 27, 2026	
Risk treatment	Turn on BitLocker on HV-AGENT-06	Chris Albright	Nov 9, 2026	
Compliance gap	Annual access privilege review for Microsoft 365 (500.7(a)(4))	Dana Whitfield	Nov 30, 2026	
Project task	Block Guest Wi-Fi from the office LAN	Chris Albright	Nov 16, 2026	
Project task	Retire the old guest Wi-Fi password and rotate the office one	Chris Albright	Dec 17, 2026	

F. Firewall and network

Open UniFi firewall and network findings (most severe first, up to 100) and the settings changes detected in the period (up to 50).

Severity	Finding	Site	Detail	Since
medium	Guest Wi-Fi can reach the office network	Main office	The Guest network has no rule blocking traffic to 192.168.10.0/24 (office LAN).	Oct 11, 2026

G. Data sources

How each area was checked. Device data counts only when a computer checked in within 30 days; identity and ticket sync data within 7 days.

Area	State	Summary
Computers and devices	Needs attention	5 device problems were found; 25 of 26 computers checked in.
Security updates	Action needed	23 of 25 scanned computers are up to date.
Security alerts and incidents	Action needed	23 alerts were raised and 21 resolved during the period. No security incident was recorded.
Tickets and requests	Needs attention	37 tickets were opened and 35 closed during the period; 6 are open now.
People: MFA, training and phishing	Action needed	MFA: 22 of 24 people. Training: 21 of 24 people current. Phishing test: 8% clicked.
Backups	Good	Every checked backup succeeded in the last 7 days.
Email security	Needs attention	8,930 messages checked, 44 flagged. Email authentication is incomplete. A domain registration expires soon.
Firewall and network	Needs attention	No urgent firewall findings; 1 setting needs attention.
Vulnerabilities	Action needed	1 critical and 3 high vulnerabilities are open on 7 computers. 1 of them has been open for more than 30 days.
Compliance	For information	Enrolled in NYDFS Cybersecurity Regulation (23 NYCRR 500).
Outstanding actions	Needs attention	7 action items are open; 1 past due.