DEMONSTRATION CHANGE RECORD

Security hardening change summary

Demonstration sample. Illustrative data, not a client report.

Fictional setup: Pine Laptop / macOS 16.1; Northstar Phone / AuroraOS 18.2; HomeMail account

Agreed scope

- Apply only owner-approved changes to account sign-in, device updates, screen lock and backup settings.
- Check everyday sign-in after each change and document the result.
- Owner enters all passwords and keeps recovery codes.
- No compromise investigation, forensic analysis, data recovery or network penetration testing.

Review methods

Changes were demonstrated and approved one at a time. The fictional owner entered credentials, stored recovery material and confirmed essential services after each step.

Findings and basis

Priority	Area	Finding	Basis
Completed	Email sign-in	Two-step verification enabled with an authenticator app.	Test sign-in and recovery prompt completed successfully.
Completed	Laptop protection	Automatic security updates and a 5-minute screen lock enabled.	Settings re-opened after restart and remained active.
Completed	Phone access	Unused cloud session signed out.	Session disappeared from the active-device list.
Deferred	Router network	Separate smart-device network not configured.	Current router model requires an on-site check before changes.

Priority recommendations

- Review active account sessions monthly for the next three months, then quarterly.
- Keep the laptop connected during its scheduled update window and verify restart prompts.
- Confirm the phone backup date after major operating-system updates.
- Schedule the router review only after documenting devices that must remain connected.

Changes completed

- Enabled authenticator-based two-step verification for the fictional email account.
- Enabled automatic security updates and a 5-minute screen lock on the fictional laptop.
- Signed out one unused fictional phone cloud session with owner approval.

Remaining actions and limitations

- Store a second copy of recovery codes in a separate owner-controlled secure location.
- Router segmentation remains pending and requires a separate agreed scope.
- Hardening reduces common risks but does not determine whether a suspected compromise occurred.

Demonstration sample. Illustrative data, not a client report.