PUBLIC SAMPLE DELIVERABLE

Security Improvement Plan

Northstar Demo Company | Prioritized actions and 12-month roadmap

Fictional public sample. Not based on a real client. This sample is not legal advice, a privacy compliance opinion, a certification determination, or a guarantee of security outcomes.

Action Plan Overview

The assessment action plan translates reviewed findings into practical work items. It is intended to support ownership, sequencing, dependency, and approval conversations after the assessment.

Action ID	Related Risk ID	Phase	Priority	Area	Action	Owner	Status
A-001	R-001	0-30 days	High	Identity	Validate privileged account MFA coverage and document exceptions.	IT Owner	Not started
A-002	R-002	0-30 days	High	Backup	Run and document one restore test for a critical system.	IT Owner	Not started
A-003	R-003	30-90 days	Medium	Endpoint	Create a device inventory with owner, encryption, and protection status.	Operations	Not started
A-004	R-004	30-90 days	Medium	Incident Response	Create a concise escalation procedure and contact matrix.	Leadership	Not started

Expected Outcomes

- Leadership has a practical tracker for the highest-value follow-up work.
- Owners can confirm whether an item needs internal action, outside support, or accepted risk.
- Status can be updated without changing the original assessment finding.

Approval and Boundary Notes

Recommendations are not production change authorization. Remediation and validation require separate written approval. Policy gaps are included only where reviewed evidence supports them.

Security Improvement Plan

Roadmap Overview

This sample roadmap sequences improvements by urgency, dependency, and practical implementation timing. It is intended to support planning conversations after assessment findings are reviewed.

Timeframe	Priority	Initiative	Owner	Dependency	Expected outcome
0-30 days	High	Validate privileged MFA coverage	IT Owner	Identity admin access	Documented control coverage for privileged accounts.
0-30 days	High	Complete one restore test	IT Owner	Backup platform and test window	Evidence-backed recovery confidence for one critical system.
30-90 days	Medium	Build practical device inventory	Operations	Endpoint data source	Owner, encryption, and protection status visible in one place.
30-90 days	Medium	Create incident escalation procedure	Leadership	Role assignments	Repeatable escalation path for common incidents.
90-365 days	Strategic	Assign SaaS owners and review admin access quarterly	Leadership	Application inventory	Clear accountability for key business systems.
90-365 days	Strategic	Create annual policy review cadence	Leadership	Policy owner list	Improved policy currency and evidence readiness.

Planning Notes

- Sequence high-priority identity and recovery work before broader maturity efforts.
- Use low-effort evidence improvements to support customer, vendor, and insurance conversations.
- Treat the roadmap as a planning aid, not an implementation authorization.