CUSTOMER DOCUMENTATION SAMPLE

Security Baseline and Improvement Roadmap

Plain language view of safeguard coverage prioritized risks owners and sequenced work

Prepared for Harborlight Design Studio | Fictional demonstration environment

This roadmap turns a sample security review into a small number of owned decisions. It records the evidence state of key safeguards, avoids exposing exploitable configuration, and separates completed controls from proposed improvements.

Document Control

CLASSIFICATION	Public fictional sample	VERSION	1.0
DOCUMENT OWNER	Tyler's Tech Company	EVIDENCE DATE	September 5 2026
REVIEW CADENCE	Quarterly and after material change	SAMPLE STATUS	Public fictional example

How to read status labels Verified, Customer confirmed, Provider reported, Planned, Out of scope, and Not verified show how evidence would be classified in a live customer document. All facts and statuses in this public sample are fictional.

Baseline Coverage

Area	Sample current state	Evidence	State
Identity	Individual accounts and multifactor authentication for covered users	Administrative readback	Verified
Privileged access	Named administrative roles separated from ordinary work	Role inventory	Verified
Endpoint protection	Managed security and device policy on covered laptops	Management console	Verified
Patching	Operating-system update policy with exception follow-up	Management reporting	Provider reported
Email protection	Microsoft 365 baseline controls and user reporting path	Configuration review	Verified
Backup and recovery	Separate covered-data copies with bounded restore evidence	Backup console and test record	Tested
Network	Managed site boundary and separated guest access	Controller readback	Verified
Employee lifecycle	Approved joiner role-change and offboarding workflow	Runbook and sample closure	Customer confirmed
Security awareness	Annual education and reporting reminder	Customer record	Not verified
Vendor access	Material vendors identified; recurring access review incomplete	Vendor register	Planned

Executive View

The sample environment has a sound operating baseline for named identities, managed devices, network administration, and covered backups. The highest-value next steps are to confirm vendor access, formalize security-awareness evidence, complete the remaining backup coverage check, and schedule an incident-response tabletop.

Prioritized Risk Register

Priority	Observation	Business effect	Recommended action	Owner	State
High	Vendor-access review is incomplete	Former or unnecessary access may remain longer than intended	Inventory material vendors and review named access quarterly	Operations and TTCo	Planned
High	Two design laptops require backup coverage confirmation	Local project files may not meet the stated recovery approach	Verify protected folders and complete a test restore	TTCo	Planned
Medium	Incident roles have not been exercised	A real event may lose time while authority and communication are clarified	Run a bounded leadership tabletop	Leadership and TTCo	Proposed
Medium	Awareness completion evidence is inconsistent	Leadership cannot confirm that the assigned activity reached every employee	Set an owner and maintain completion evidence	Operations	Proposed
Low	Core switch is nearing the preferred support horizon	Failure may require expedited replacement	Approve the planned lifecycle refresh	Operations	Proposed

Improvement Roadmap

Horizon	Action	Completion evidence	Decision owner
30 days	Confirm backup enrollment and protected folders for two design laptops	Coverage readback and representative restore	Operations
30 days	Complete the material vendor and access-owner inventory	Approved vendor-access register	Operations
60 days	Implement the quarterly vendor-access review	First signed review with exceptions	Leadership
90 days	Run an incident-response tabletop focused on account compromise and file recovery	Scenario record decisions and follow-up actions	Leadership
90 days	Establish awareness completion evidence	Assigned owner schedule and completion record	Operations
12 months	Review privileged access device lifecycle recovery evidence and insurance requirements	Annual baseline review	Leadership and TTCo

Decision and Deferral Log

Decision	Current position	Owner	Review date
Vendor-access review cadence	Quarterly review proposed; leadership approval pending	Leadership	October 2026
Incident tabletop scope	Account compromise and file recovery scenario proposed	Operations	November 2026
Core switch replacement	Budget request planned for Q4	Operations	October 2026
Personal-device management	Out of scope under current service order	Leadership	At service renewal

Evidence and Limits

- The public sample uses generalized observations and does not include raw scan output, exact configuration, hostnames, firewall rules, administrator endpoints, or active weaknesses.
- A green administrative dashboard is evidence about the reported state of that control; it is not proof that every device user or recovery scenario is covered.
- This roadmap is not a compliance certification penetration test incident-response retainer or guarantee against loss.
- Regulatory contractual and insurance requirements require separate confirmation for the actual customer and engagement.

Review Method

At each quarterly review, close completed actions only after readback or test evidence is recorded. Carry forward deferred actions with the deciding owner and date. Reprioritize when the business adds people, systems, locations, regulated data, or material vendors.

Revision History

Version	Date	Change	Prepared by
1.0	September 2026	Public sample release	Tyler's Tech Company