

BLACKTECHSTARTUP EDUCATION

Startup Security & Privacy Baseline Before Enterprise Sales or Fundraising

Build a stage-appropriate baseline for data inventory, MFA/access, credentials, backups, vendors, privacy and incident response—and keep evidence that proves the controls exist.

Security readiness is evidence-based. CISA recommends MFA and tested backups for small businesses; FTC guidance emphasizes limiting sensitive-data access and protecting only data you have a legitimate reason to keep; NIST's Privacy Framework starts with understanding and managing privacy risk. For a startup, the baseline is not a giant policy binder—it is a small set of real controls, named owners and proof.

Know what weak and strong look like

READINESS AREA	WEAK / DILIGENCE RISK	STRONG / INVESTOR-READY
Data	No inventory; "we use cloud providers."	Sensitive/customer/business data types, systems, owners, flows and retention documented.
Access	Shared admin accounts or password-only critical systems.	Named accounts, MFA, least privilege, periodic admin review and offboarding.
Secrets	API keys in chat/repos/local files.	Secret manager/environment controls, rotation and incident process.
Backups	Provider says data is replicated.	Critical data backups/restores tested; RPO/RTO expectations documented.
Incident	Founder will "handle it."	Detection/escalation contacts, containment steps, customer/legal notification decision path and evidence preservation defined.

Inventory before buying tools

List data categories and critical systems. Mark customer PII, credentials, financial data, source code, model/data assets and regulated data. Delete collection/storage you do not need.

Lock identity and admin access

MFA on email, cloud, source control, production, database, finance and cap-table systems. Eliminate shared accounts. Review privileged access on a schedule and remove access immediately on departure.

Protect secrets and production changes

Store keys/tokens outside source code; restrict production deployment; log/admin events where practical; separate environments; rotate credentials after exposure or personnel changes.

Prove recovery

Back up critical data/configuration and actually restore it. Know what the SaaS vendor backs up versus what you are responsible for. Record test date and outcome.

Prepare the evidence pack

Keep security overview, architecture/data-flow diagram, access-control statement, backup/restore evidence, vendor list, incident plan, privacy policy/data retention and remediation log. Answer questionnaires from evidence instead of reinventing answers each sale.

Run the diligence stress test before investors do

Do not rehearse an answer. Rehearse the evidence. Give yourself a short diligence window and try to produce the underlying records without rebuilding the story from memory. A clean result is reproducible, tied to a source system or signed document, and consistent with the numbers elsewhere in the company.

→ **Data:** Put the underlying records on screen and prove this standard:
Sensitive/customer/business data types, systems, owners, flows and retention documented. If the evidence still looks like this weak state—No inventory; “we use cloud providers.”—record the gap, name an owner and give it a due date instead of explaining it away.

→ **Access:** Put the underlying records on screen and prove this standard: Named accounts, MFA, least privilege, periodic admin review and offboarding. If the evidence still looks like this weak state—Shared admin accounts or password-only critical systems.—record the gap, name an owner and give it a due date instead of explaining it away.

→ **Secrets:** Put the underlying records on screen and prove this standard: Secret manager/environment controls, rotation and incident process. If the evidence still looks like this weak state—API keys in chat/repos/local files.—record the gap, name an owner and give it a due date instead of explaining it away.

→ **Backups:** Put the underlying records on screen and prove this standard: Critical data backups/restores tested; RPO/RTO expectations documented. If the evidence still looks like this weak state—Provider says data is replicated.—record the gap, name an owner and give it a due date instead of explaining it away.

→ **Incident:** Put the underlying records on screen and prove this standard: Detection/escalation contacts, containment steps, customer/legal notification decision path and evidence preservation defined. If the evidence still looks like this weak state—Founder will “handle it.”—record the gap, name an owner and give it a due date instead of explaining it away.

Do the math investors will do

Stage-appropriate risk rule: prioritize controls by $\text{impact} \times \text{likelihood} \times \text{exposure}$. A five-person B2B startup handling customer credentials should fix shared admin access before buying a complex governance platform. Evidence of a simple control that works is stronger than a 40-page policy nobody follows.

Build the evidence investors can verify

✓ Data/system inventory and flow diagram

✓ MFA/privileged-access review evidence

✓ Secret-management and key-rotation process

✓ Backup/restore test log

✓ Critical vendor inventory/risk review

- ✓ Privacy notice/retention and deletion practices
- ✓ Incident response contacts/playbook/tabletop record
- ✓ Security overview for enterprise/investor diligence

Questions an investor may ask

- ? Where is customer data stored and who can access it?
- ? Which critical accounts still lack phishing-resistant MFA?
- ? When was the last restore test?
- ? What happens in the first hour after a credential leak?
- ? Which vendor failure would stop service or expose customer data?

30-day repair sprint

- 1 Days 1–3: inventory systems/data and critical accounts.
- 2 Days 4–7: enforce MFA/least privilege and remove shared credentials.
- 3 Days 8–12: move/rotate secrets and harden production access.
- 4 Days 13–17: test backup/restore.
- 5 Days 18–23: review vendors/privacy/retention.
- 6 Days 24–30: run an incident tabletop and assemble the evidence pack.

Research behind this guide

Use the primary and authoritative sources below to verify current rules, market conditions and technical guidance. Terms and regulations can change.

CISA — Cyber Guidance for Small Businesses



FTC — Start With Security



FTC — Data Security Guidance



NIST — Privacy Framework



Important: This guide is educational information, not individualized legal, tax, investment, employment, security or compliance advice. For decisions with material legal or financial consequences, use a qualified professional who can review your facts.

SHARE THIS GUIDE ↗

POWERED BY: BLACK TECH STARTUP

blacktechstartup.com