Startup Security Checklist

One-page, pragmatic controls for Seed–Series B teams

Company | Security Owner | Target Date

First 10 to Ship

- [ ] Name a security owner and simple RACI
  One accountable person; delegate tasks with owners.
- [ ] SSO everywhere + enforce MFA
  All apps via IdP; block legacy auth; require MFA for admins.
- [ ] Production/admin access hardening
  Hardware keys (preferred), per-user accounts, just-in-time elevation.
- [ ] Password manager + secrets management
  Company-wide vault; rotate shared creds; no secrets in code.
- [ ] Laptop baseline via MDM
  Disk encryption, screen lock, auto updates, EDR deployed.
- [ ] Cloud baseline
  Disable root keys, CIS benchmark, tag owners, log to a central account.
- [ ] Backups + quarterly restore test
  Encrypt, isolate, and test restores for prod data & infra.
- [ ] Secure SDLC guardrails
  Branch protection, code review, dependency & secret scanning in CI.
- [ ] Incident response ready
  On-call, contact tree, 60-minute tabletop, customer comms template.
- [ ] Vendor risk intake
  Lightweight questionnaire, DPA templates, owner for each vendor.

Foundations

- [ ] Data inventory & retention
  Identify PII/PHI; define lawful basis; set retention & deletion.
- [ ] Logging & detection
  Centralize logs, basic alerts on auth, admin, and data access.
- [ ] Environment separation
  Prod vs. non-prod isolation; least-privilege roles; service accounts.
- [ ] Policies that people actually read
  Acceptable use, access, incident, change, vendor—one page each.
- [ ] Customer readiness
  Security page, shortlist of controls, and a sane NDA/DPA process.

Map to frameworks (fast)

SOC 2 CC7 / CC6	IR tabletop, logging/alerts, access reviews, change control.
ISO 27001 Annex A	Device mgmt, backups, cryptography, supplier security.
AI & data features	Add data-handling rules and model secrets to the SDLC checks.