Trust Center Checklist

A practical 40-item checklist for launching and maintaining a SaaS trust center buyers actually trust. By VendorLens — vendorlens.io

1. Foundations

- Decide which buyer questions you want the trust center to answer (security, privacy, compliance, subprocessors).
- Pick a public URL: trust.yourdomain.com (preferred) or yourdomain.com/trust.
- Confirm a single owner for the page (usually security, ops, or founder).
- Write a one-paragraph plain-English overview of your security posture.
- Add a security@ contact email and a vulnerability reporting note.

2. Documents to publish (or gate behind NDA)

- SOC 2 Type II report (NDA-gated if applicable).
- ISO 27001 certificate (public) and Statement of Applicability (gated).
- Penetration test summary letter (public) and full report (gated).
- Latest security whitepaper / overview.
- Data Processing Agreement (DPA) template.
- Standard Contractual Clauses (SCCs) where relevant.
- Privacy policy and Terms of Service (public links).
- Business Continuity / Disaster Recovery summary.
- Subprocessor list with last updated date.

3. Required content sections

- Compliance & certifications badges (with last audit date).
- Encryption in transit and at rest (algorithms and key management).
- Authentication options (SSO/SAML, MFA, password policy).
- Access control model and least-privilege practices.
- Logging, monitoring, and incident response summary.
- Backup, RPO and RTO commitments.
- Vulnerability management and pen-test cadence.
- Employee security: background checks, training, offboarding.
- Hosting region(s) and data residency options.

4. Access control & gating

- Public tier: marketing-friendly overview, certs, subprocessors.
- Email-gated tier: whitepapers, architecture diagrams.
- NDA-gated tier: SOC 2 report, pen-test report, SOC 2 bridge letter.
- Time-limited access tokens (24–72 hours).
- Watermarking on PDFs with requester email.

- Auto-expire access after document download.

5. Buyer experience

- Search bar across documents and FAQs.
- FAQ section covering the top 10 procurement questions.
- Clear CTA: request access / contact security team.
- Mobile-friendly layout (procurement opens links on phones).
- Live status indicator or link to status page.

6. Operations & maintenance

- Quarterly review cadence for every document.
- Subprocessor changes notified to customers in advance.
- Audit log of who accessed which document and when.
- Single source of truth — no scattered Google Drive links.
- Sales playbook: send the trust portal link before the questionnaire.

7. Bonus — to stand out

- Plain-English summaries on top of each long-form doc.
- Compliance roadmap (what's planned for next 6–12 months).
- Customer logos under an NDA list (with permission).
- Direct booking link to your security lead.
- RSS / changelog of trust center updates.