

# Mini Trust Center Kit Guide

A practical setup guide for early SaaS and AI teams that need clearer security questionnaire, procurement portal, subprocessor, policy, and trust-center documentation before formal certification.

## Best for

Pre-seed and seed  
B2B software teams

## Setup time

30-60 minutes for a  
first pass

## Important limit

Templates, not  
certification or advice

---

## Start Here

1. Open `templates/security-overview-one-page.md` and replace every bracketed placeholder.
2. Open `templates/subprocessors-register.csv` and list only vendors you actually use.
3. Use `templates/procurement-portal-intake-tracker.csv` to log buyer portal questions, evidence sources, owners, due dates, and review status.
4. Use `templates/security-questionnaire-answer-bank.md` to draft buyer answers.
5. Publish `trust-center-site/index.html` only after every statement is true.
6. Keep a copy of the final packet in a shared internal folder for future buyer requests.

## Buyer Packet

Document	When to Send
One-page security overview	When a buyer asks for a security summary or procurement packet.

Procurement portal intake tracker	When a buyer sends a portal, spreadsheet, or long email thread with owners and due dates to manage.
Subprocessor register	When a buyer asks which vendors process customer data.
Questionnaire answer bank	When filling security questionnaires or vendor review forms.
SOC 2 roadmap language	When a buyer asks whether you are SOC 2 certified.
AI/data-use disclosure	When your product includes AI features or AI vendors.

## Claims Safety Checklist

- No claim of SOC 2 certification unless you have a current report.
- No claim of HIPAA, GDPR, or privacy-law compliance without qualified review.
- No promise that incidents cannot happen.
- No vendor listed unless you actually use it.
- No security control listed as implemented unless it is actually implemented.

## Important Disclaimer

This kit is a documentation template pack. It is not legal advice, cybersecurity advice, SOC 2 certification, audit readiness, HIPAA compliance, GDPR compliance, or a guarantee that incidents cannot happen.