FREE CHECKLIST

Trust Center Document Checklist

Every section and document a customer-facing trust center needs, with guidance on what to publish openly, what to share only under NDA, and what not to claim.

1. Overview

Item	What it should contain	Publish / Gate	Owner	Ready? (Y/N)
Security overview	Plain-language summary of how you protect customer data	Publish		
Security contact	Monitored address for security questions and vulnerability reports	Publish		
Last-updated date	Date the page was last reviewed	Publish		

2. Compliance status

Item	What it should contain	Publish / Gate	Owner	Ready? (Y/N)
Frameworks you follow	Only frameworks you actually follow, with accurate status: 'aligned with', 'in progress', or 'certified' (only if a current certificate exists)	Publish		
Audit reports (SOC 2, ISO certificate)	The report or certificate itself — only if issued and current	Gate (NDA)		
Bridge letter	Covers the gap between report period end and today	Gate (NDA)		
Self-assessments (CAIQ, SIG Lite)	Completed questionnaire answers	Gate		

3. Policies

Item	What it should contain	Publish / Gate	Owner	Ready? (Y/N)
Information security policy	Summary publicly; full policy on request	Summary publish / full gate		
Acceptable use, access control, encryption	Short summaries of each	Publish summary		
Incident response plan	Summary of process and customer notification timelines	Publish summary		

Business continuity / DR	Recovery objectives and test cadence	Gate		
Vendor management policy	How sub-processors are assessed	Publish summary		

4. Data protection

Item	What it should contain	Publish / Gate	Owner	Ready? (Y/N)
Data types processed	What customer data you hold and why	Publish		
Data location and hosting	Regions and hosting providers	Publish		
Encryption	In transit and at rest, key management summary	Publish		
Retention and deletion	Retention periods and deletion on termination	Publish		
Data Processing Agreement (DPA)	Standard DPA customers can sign	Publish or on request		

5. Sub-processors

Item	What it should contain	Publish / Gate	Owner	Ready? (Y/N)
Sub-processor list	Name, purpose, location for each	Publish		
Change notification	How customers are told about new sub-processors	Publish		

6. Product and infrastructure security

Item	What it should contain	Publish / Gate	Owner	Ready? (Y/N)
Access control and SSO/MFA	How staff and customer access is controlled	Publish		
Logging and monitoring	What is logged and how alerts are handled	Publish summary		
Vulnerability management	Scanning cadence and patch SLAs	Publish summary		
Penetration test summary	Executive summary of latest test	Gate (NDA)		

7. Corporate security

Item	What it should contain	Publish / Gate	Owner	Ready? (Y/N)
Employee security training	Frequency and topics	Publish		

Background checks	Where lawful and applicable	Publish		
Cyber insurance	Certificate of insurance	Gate		

8. Do-not-claim list

Wording to avoid	Use instead
'SOC 2 certified' (SOC 2 is an attestation report, not a certification)	'SOC 2 Type II report available under NDA' — only once issued
Badges or logos for audits not completed	Status text: 'SOC 2 readiness in progress'
'Fully compliant with HIPAA / GDPR'	'Our controls are designed to support HIPAA / GDPR requirements'
'Bank-grade' or 'military-grade' security	Name the actual control, e.g. 'AES-256 encryption at rest'

9. Upkeep

Task	Frequency
Review every page section	Quarterly
Update sub-processor list	On every change
Replace expired reports / certificates	On issue
Check every claim still matches reality	Quarterly

> Want this done for you? See Trust Center Consulting at quantumauditengine.com/trust-center-consulting/. This checklist is general guidance, not legal advice.