# Trust center best practices checklist

One page. Public layer, gated layer, and the operational habits that keep both accurate.
Reviewed 11 August 2026 by Rania Zouari, VendorLens · vendorlens.io/guides/what-to-include-in-a-trust-center

## PUBLIC LAYER

- [ ] Plain-language posture summary
- [ ] Certification status with issuer, scope and period
- [ ] Hosting regions and residency options
- [ ] Dated subprocessor list as page content
- [ ] Monitored security contact address
- [ ] Vulnerability disclosure route
- [ ] Privacy notice and DPA template

## GATED LAYER

- [ ] SOC 2 report and bridge letter behind an NDA
- [ ] Full pen-test report and architecture diagrams behind an NDA
- [ ] Policy pack and SoA released on request
- [ ] Time-limited links on every approved request
- [ ] Watermarking on downloaded PDFs

## OPERATIONS

- [ ] One named owner and one deputy
- [ ] Quarterly content review in the calendar
- [ ] Date shown on every artefact
- [ ] Access log reviewed monthly
- [ ] Trust-center update included in infrastructure and subprocessor changes

### How to use this page

1. Tick what is already published. Anything unticked in the public layer is a question you are still answering by email.

2. Decide a default access posture per document class once, and write it down, rather than deciding per deal.

3. Put a date on every artefact and a named owner on the page. Freshness is what a returning reviewer checks first.

4. Re-run this checklist quarterly, and after any change to hosting, subprocessors or certification scope.