Vendor review document pack

A 30-item template for assembling the security evidence enterprise buyers request during a vendor review - and for recording who owns each document, when it expires and who may see it. Process guidance only: this template contains no legal or contractual wording.

1. Audit reports and certificates

The items reviewers look for first. Record the period or validity dates, not just the file.

- [ ] SOC 2 report (note Type 1 or Type 2, and the audit period covered).
- [ ] Bridge letter, if the current audit period has not closed yet.
- [ ] ISO 27001 certificate, with certificate number and expiry date.
- [ ] ISO 27001 Statement of Applicability, if you share it.
- [ ] Any sector or regional certification your buyers ask about.

2. Technical assurance

Evidence about testing and architecture rather than about the management system.

- [ ] Penetration-test summary from the most recent test, in shareable form.
- [ ] Remediation note covering findings from that test, if you publish one.
- [ ] Security overview or whitepaper: encryption, access control, logging, hosting.
- [ ] Vulnerability-management and patching summary.
- [ ] Architecture or data-flow diagram, if your buyers request one.

3. Data protection and legal

Usually the items that can be published openly.

- [ ] Data processing agreement, with its current version date.
- [ ] Privacy policy.
- [ ] Subprocessor list with purpose, entity and hosting region, plus last-updated date.
- [ ] Data-retention and deletion summary.
- [ ] International transfer mechanism, where relevant to your buyers.

4. Operational resilience

Asked for in most enterprise reviews and in nearly all reassessments.

- [ ] Business continuity and disaster-recovery summary, with stated RPO and RTO.
- [ ] Incident-response summary, including notification commitments.
- [ ] Backup approach and last restore test date.
- [ ] Status page or uptime history reference.
- [ ] Insurance certificate, where your buyers require it.

5. For every item, record

This is what turns a folder into a maintainable pack.

- [ ] Owner: the person responsible for keeping it current.
- [ ] Effective date or version, and the date it next needs refreshing.
- [ ] Access rule: open on the portal, or restricted behind a request and NDA.
- [ ] Whether restricted copies should be watermarked with the requester.
- [ ] Default access window, and who may extend it.

6. Deliberately not in the pack

Keeping these out is part of the design.

- [ ] Raw penetration-test output and unredacted findings.
- [ ] Draft policies and unapproved documents.
- [ ] Internal risk registers and audit working papers.
- [ ] Customer-specific material belonging to another customer.
- [ ] Anything you cannot commit to keeping current.

How to use it: work section by section and fill in the owner, effective date and access rule for each item you actually hold. Gaps are useful information - they are the questions a buyer will ask that you cannot yet answer from a document.