WRIGHTBRAINED
SECURITY

FREE CHECKLIST · SUPPLY CHAIN

Security Terms for Vendor Contracts

What to put in writing before a vendor touches your data or your systems: baseline protections, incident notice, your right to check, and what happens to your data at the end.

Your contract is a security control

Most companies know what their suppliers say about security. Few have it in writing, and fewer have the right to check. These are the terms we look for in supplier reviews. Check off what your current contracts already cover.

> **Match the terms to the risk.** An office-supply vendor doesn't need all of this. A vendor that holds your data or can reach your network does.

Before you sign

- [ ] **Know what they will touch.** Write down whether this vendor gets your data, access to your systems, or neither. It decides how many of the terms below you need.
- [ ] **Ask for evidence, not promises.** A certification, an independent assessment report, or a signed attestation you can keep on file.
- [ ] **Ask who else is involved.** Which subcontractors or cloud providers will handle your data or reach your systems.

Security basics in the contract

- [ ] **Baseline protections.** Multi-factor authentication for email, remote access and admin accounts; centrally managed, patched computers; and monitoring for attacks.
- [ ] **Access limits.** Named accounts only, the least access needed, remote access through approved methods, and access removed promptly when their people leave.
- [ ] **Keep it current.** They keep these protections in place for the whole contract, not just on the day they answered your questionnaire.

When something goes wrong

- [ ] **Incident notice with a clock.** They tell you within a set time (for example 72 hours, which matches DoD reporting under DFARS 252.204-7012) and name who they will contact.
- [ ] **Cooperation.** They help with your investigation, share what they know, and preserve logs and evidence.
- [ ] **Who pays.** Responsibility for breach costs, notification costs and cleanup when the incident is on their side, backed by cyber insurance with stated limits.

Your right to check

- [ ] **Evidence on request.** Annual attestation or current certification, and the right to ask for supporting evidence.
- [ ] **Assessment rights.** The right to review their security (by you or someone you choose) with reasonable notice.
- [ ] **Material changes.** They tell you about significant changes, such as a new hosting provider, an acquisition, or losing a certification.

Your data

- [ ] **Where it lives.** Where your data is stored and processed, including country, and that it is encrypted in transit and at rest.
- [ ] **Use limits.** They use your data only to deliver the service, not to train products or share with others.
- [ ] **At the end.** Return or destruction of your data when the contract ends, with written confirmation.

Industry-specific

- [ ] **Defense work.** Flow down DFARS 252.204-7012 (and 252.204-7021 for CMMC) when they will handle CUI. Cloud services holding CUI need FedRAMP Moderate or equivalent.
- [ ] **Patient data.** A signed HIPAA agreement (a BAA) before they receive any patient information.
- [ ] **Their suppliers.** They pass the same requirements to their own subcontractors who touch your data.

This checklist is a starting point for a conversation with your legal counsel, not legal advice or contract language.

Want a second set of eyes?

We're assessors. We find the gaps, direct the fix, and check that it holds. **wrightbrainedsecurity.com/contact** · jil@wrightbrainedsecurity.com