

Vulcan and DFARS 252.204-7012

Last updated September 29, 2026. Blacksmith AI LLC, Vulcan at vulcan.blacksmithai.net. The live copy is at <https://www.blacksmithai.net/security/dfars-7012>.

Defense contractors who handle Controlled Unclassified Information carry DFARS 252.204-7012 obligations, and when they use a cloud service for that information the clause reaches the service provider. This page states plainly what Vulcan is, what it holds, and what Blacksmith AI commits to, so your compliance lead can place Vulcan in your system security plan without guessing.

1. What Vulcan is

Vulcan is a commercial software-as-a-service product for government contracting teams: contract search, proposal writing, a company library and a pursuit pipeline. In DFARS terms Blacksmith AI LLC is an external cloud service provider. Vulcan is not a FedRAMP-authorized service and holds no FedRAMP Moderate equivalency; if your contract requires one for CUI, Vulcan is not the place for that CUI.

2. What Vulcan stores, and where

- Your account, organization, pursuit, proposal, contact and chat records: MongoDB Atlas, AWS us-east-1, encrypted at rest.
- Files you upload and the text extracted from them: MongoDB Atlas (GridFS) and Amazon S3, us-east-1, encrypted at rest, S3 versioned.
- Search embeddings of your documents: Pinecone, United States, one namespace per organization.
- Short-lived cache and queue entries: Redis Cloud, us-east-1. Nothing is kept only there.
- Text sent to AI providers (Anthropic, OpenAI, Perplexity) for the task you ask for, under API terms that exclude model training; the full list is on the security page.

3. What Vulcan does not store

- Card numbers: Stripe holds them; they never reach our servers.
- Passwords in clear: only bcrypt hashes.
- Credentials for apps you connect, in clear: they are encrypted with AES-256-GCM before storage.
- Classified information of any level. Vulcan is not accredited for it and must not receive it.

4. Cyber incident reporting: the 72-hour commitment

If Blacksmith AI discovers a cyber incident that affects your data in Vulcan, we notify the organization owner at the email on the account within 72 hours of discovery, with what happened, what data was involved, what we have done, and a named contact. That is the window DFARS 252.204-7012(c) gives you to report to DoD through DIBNet, and our notice is written so you can file from it. Our incident response plan, with the customer notice template, is kept in the repository and available on request.

5. Media preservation and forensic access

- On notice of an incident we preserve the affected records, files, server logs and database snapshots for at least 90 days from the report, and longer on your written request.
- On your written request, or DoD's through you, we give access to that preserved material and to the people who handled the incident, for damage assessment or forensic analysis.
- Server logs are kept 365 days in normal operation, and database snapshots up to a year, so preservation starts from a full record.

6. Subprocessors and flow-down

Every outside service that can receive your data is named on the security page with its purpose, data category and region, and the list is generated from the credentials our production servers hold so it cannot go stale. Each is engaged under terms that limit its use of the data to providing its service and prohibit training on it. We give 30 days' notice before a new subprocessor processes customer content.

7. Export-controlled technical data

Production access to Vulcan's infrastructure and data is held only by U.S. persons, as defined in 22 CFR 120.62. ITAR-controlled technical data is still out of scope of the service: do not upload it to Vulcan. The documents you upload are processed by the AI providers on our subprocessor list, which are not ITAR-restricted environments.

8. CMMC status

Vulcan makes no CMMC certification claim. The CMMC program's Phase 2 was suspended on 13 July 2026 (Class Deviation 2026-O0025 Rev 3, 3 September 2026). Our controls are designed against NIST SP 800-171; that is a design target, not an assessed status. No SOC 2 report or third-party penetration test exists yet; both are planned when a customer contract calls for them.

9. Who to ask

Blacksmith AI LLC, 1611 N Broadway Ave, Oklahoma City, OK 73103. security@blacksmithai.net. Security questionnaires are answered from the same facts as this page; ask and we will fill yours in.

Blacksmith AI LLC · 1611 N. Broadway Ave., Oklahoma City, OK 73103, United States · info@blacksmithai.net · <https://www.blacksmithai.net>