How does Cyber Crucible handle data retention and deletion?

Short answer: Cyber Crucible minimizes what it holds and retains data only as long as necessary to provide the service. It never collects customer content, credentials, or keys in the first place, so the highest-risk categories have nothing to retain. Behavioral telemetry and derived security metadata are aged off on defined schedules, and at the end of a contract all associated data is made available for deletion with confirmation.

The principle

- **Minimize first.** The most sensitive data is never collected, so there is nothing in those categories to retain or destroy.
- **Retain by purpose.** Behavioral telemetry and security metadata are kept only as long as they serve detection, investigation, and reporting, then aged off.
- **Delete on exit.** At end of contract, associated data is made available for deletion and Cyber Crucible provides confirmation.

What is documented

A documented destruction process covers both printed and electronic information. The specific retention periods by data type are provided to reviewers under NDA, and can be tightened by contract.

Revision #2
Created 2026-07-23 15:18:13 UTC by Dennis Underwood
Updated 2026-07-23 18:19:45 UTC by Dennis Underwood