What is the Cyber Crucible Mutual NDA, and who is bound by it?

Short answer: It is a binding mutual non-disclosure agreement that every Cyber Crucible employee, contractor, and vendor with potential access to customer operational data or management systems must execute **before onboarding**. It is published at cybercrucible.com/mutualNDA.

Who signs it

All personnel with potential access to customer operational data or management systems are legally bound prior to onboarding. That includes employees, contractors, and vendors — not just staff.

Why "mutual" matters

A one-way NDA protects only the vendor. A mutual agreement binds Cyber Crucible to protect *your* confidential information on the same terms it expects for its own. For a security vendor whose personnel may see operational detail about your environment, that symmetry is the point.

How it fits with the other controls

The NDA is the contractual layer of a broader insider-risk posture:

- **Contractual** — binding mutual NDA before any access is granted.
- **Access** — administrative access to customer management instances restricted to vetted personnel, strictly need-to-know, only when required for a validated business or support operation.
- **Disengagement** — if any supplier, vendor, contractor, or employee poses a security, privacy, or intellectual property risk, Cyber Crucible actively manages and isolates that risk or disengages the resource immediately.

The NDA establishes the obligation. The access controls limit how much any one person could misuse. The disengagement mandate is what makes both enforceable in practice.

Revision #2
Created 2026-07-21 18:59:56 UTC by Dennis Underwood
Updated 2026-07-21 19:33:04 UTC by Dennis Underwood