

How does Cyber Crucible manage supply chain and insider risk?

Short answer: Through binding mutual NDAs for all personnel with potential access, strictly need-to-know administrative access limited to vetted staff, and a zero-tolerance mandate to isolate or immediately disengage any supplier, vendor, contractor, or employee who poses a risk to customers or their intellectual property.

The controls

- **Mandatory non-disclosure agreements** — all personnel with potential access to customer operational data or management systems are legally bound by a mutual NDA prior to onboarding.
- **Strict need-to-know access** — administrative access to customer management instances is restricted exclusively to vetted personnel, and only when required to accomplish a validated business or support operation.
- **Vendor and resource disengagement mandate** — if any supplier, software vendor, contractor, or employee poses a security, privacy, or intellectual property risk to customers, Cyber Crucible actively manages and isolates that risk or disengages the resource immediately.

Why insider and supply chain risk belong together

Both are the same problem viewed from different angles: someone with legitimate access being the vector. Controlling it requires limiting who has access, binding them contractually, and being willing to sever a relationship quickly when risk appears — including a commercial relationship.

The disengagement mandate is the part organizations most often lack. Contracts and NDAs establish obligations; the willingness to terminate a supplier immediately is what makes them meaningful.