

Legal & Trust Documents

Where to find Cyber Crucible's agreements and trust documentation — mutual NDA, MSA and EULA, service level agreement, data processing agreements, and compliance evidence.

- [Where can I find Cyber Crucible's legal and trust documents?](#)
- [What is the Cyber Crucible Mutual NDA, and who is bound by it?](#)
- [What do the MSA and EULA cover?](#)
- [What does the Service Level Agreement cover?](#)
- [How do I complete a security questionnaire or vendor risk assessment for Cyber Crucible?](#)

Where can I find Cyber Crucible's legal and trust documents?

Short answer: Public agreements are published on cybercrucible.com — the Mutual NDA, MSA & EULA, Service Level Agreement, Privacy Policy, and Terms of Service. Compliance documentation that is provided on request — Standard Contractual Clauses, Transfer Risk Assessment, and Data Processing Agreements — comes from **dpo@cybercrucible.com**.

Publicly available

Document	Location
Mutual Non-Disclosure Agreement	cybercrucible.com/mutualNDA
Master Services Agreement & EULA	cybercrucible.com/msa-and-eula
Service Level Agreement	cybercrucible.com/service-level-agreement
Privacy Policy	cybercrucible.com/privacy-policy
Terms of Service	cybercrucible.com/terms-of-service

Provided on request

Contact **dpo@cybercrucible.com** for:

- Standard Contractual Clauses, including the SDAIA pre-approved clauses for Saudi transfers
- Transfer Risk Assessment
- Data Processing Agreement
- Data governance and sharing policy documentation

These are provided subject to reasonable confidentiality measures.

Why these are worth reading before procurement

Security vendors are unusual in that the product runs with the deepest privileges on your systems and the contract governs what the vendor may do with what it sees. The agreements above define both. The data governance material in particular answers the question most security questionnaires ask indirectly: *what does this vendor actually collect, and where does it go?*

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.

What do the MSA and EULA cover?

Short answer: The Master Services Agreement governs the commercial relationship — services, obligations, liability, and term. The End User License Agreement governs use of the software itself, including the licensing scope, which applies to compiled object code rather than source.

Key points worth knowing before signing

- **Licensing scope** — rights granted apply to the compiled object-code form of the software. The agreement does not grant rights to obtain or use source code.
- **No implied licenses** — Cyber Crucible retains all right, title, and interest in the services, documentation, and associated intellectual property. Nothing is granted by implication.
- **Implementation services** — configuration, customization, personnel training, or technical support are set out in an Order Form rather than assumed.
- **Confidentiality** — both parties may access the other's confidential information; each remains the property of the disclosing party.

Where to read it

The full agreement is published at cybercrucible.com/msa-and-eula. This page is a summary for orientation, not a substitute — the published agreement governs.

What does the Service Level Agreement cover?

Short answer: The SLA defines the service commitments Cyber Crucible makes to customers — availability, support responsiveness, and the associated terms. It is published at cybercrucible.com/service-level-agreement.

How the SLA relates to the product's design

Worth noting for anyone evaluating: because prevention happens autonomously on the endpoint in typically under 200 milliseconds, protection does not depend on service availability the way a cloud-analytics product does.

An endpoint whose management server is unreachable — or which is deliberately air-gapped — is still fully protected. Threat evaluation and process interdiction are local. Management-plane availability affects reporting and administration, not defence.

That is a meaningful distinction when comparing SLAs across vendors. For a cloud-dependent tool, management-plane downtime can mean reduced or absent protection. Here it does not.

Where to read it

The full agreement is at cybercrucible.com/service-level-agreement. Support responsiveness commitments and any environment-specific terms should be confirmed with your Cyber Crucible representative.

How do I complete a security questionnaire or vendor risk assessment for Cyber Crucible?

Short answer: Most questions are answered by the data governance material — what is collected, what is never collected, how it is protected in transit, where it is processed, and what deployment models are available. For anything requiring signed documentation, contact dpo@cybercrucible.com.

The answers most questionnaires need

Typical question	Where it's answered
What customer data does the vendor collect?	<i>What data does Cyber Crucible collect — and what does it never collect?</i>
Is data shared with or sold to third parties?	<i>Does Cyber Crucible sell or share customer data with third parties?</i>
How is data encrypted in transit?	<i>How is Cyber Crucible data protected in transit?</i>
Where is data processed and stored?	<i>Where is my data processed, and can it stay inside my country?</i>
Sub-processors and supply chain controls?	<i>How does Cyber Crucible manage supply chain and insider risk?</i>
Third-party or foreign code components?	<i>Does Cyber Crucible embed third-party libraries or foreign code?</i>
Controller or processor role?	<i>Is Cyber Crucible a data controller or a data processor?</i>
Cross-border transfer mechanism?	<i>How are cross-border data transfers handled?</i>

Two answers that commonly surprise reviewers

On certifications: Cyber Crucible's security programme is aligned with recognized industry frameworks but **does not currently hold ISO 27001 or SOC 2 certification**. If your process requires certified evidence, raise it early rather than late.

On data disclosure: because encryption keys, credentials, and customer files are never collected, there is nothing in those categories to disclose to any party — including under legal process. Several questionnaire items about disclosure, retention, and deletion are answered by the absence of collection rather than by a control.

Anything not covered

Contact **dpo@cybercrucible.com** with the specific requirement, your jurisdiction, and which deployment model you are evaluating.