Rechts- und Vertrauensdokumente

Wo Sie die Vereinbarungen und Vertrauensdokumentation von Cyber Crucible finden — gegenseitige NDA, MSA und EULA, Service-Level-Agreement, Datenverarbeitungsvereinbarungen und Compliance-Nachweise.

Wo finde ich die rechtlichen Dokumente und Vertrauensnachweise von Cyber Crucible?

Kurze Antwort: Öffentliche Vereinbarungen werden auf cybercrucible.com veröffentlicht — die Mutual NDA, MSA & EULA, das Service Level Agreement, die Datenschutzrichtlinie und die Nutzungsbedingungen. Compliance-Dokumentation, die auf Anfrage bereitgestellt wird — Standardvertragsklauseln, Transfer Risk Assessment und Auftragsverarbeitungsverträge — erhalten Sie über **dpo@cybercrucible.com**.

Öffentlich verfügbar

Dokument	Fundort
Mutual Non-Disclosure Agreement	cybercrucible.com/mutualNDA
Master Services Agreement & EULA	cybercrucible.com/msa-and-eula
Service Level Agreement	cybercrucible.com/service-level-agreement
Datenschutzrichtlinie	cybercrucible.com/privacy-policy
Nutzungsbedingungen	cybercrucible.com/terms-of-service

Auf Anfrage bereitgestellt

Wenden Sie sich an **dpo@cybercrucible.com** für:

- Standardvertragsklauseln, einschließlich der von der SDAIA vorab genehmigten Klauseln für saudische Datenübermittlungen
- Transfer Risk Assessment
- Auftragsverarbeitungsvertrag
- Dokumentation zur Data Governance und zu Richtlinien für die Datenweitergabe

Diese werden vorbehaltlich angemessener Vertraulichkeitsmaßnahmen bereitgestellt.

Warum es sich lohnt, diese Dokumente vor der Beschaffung zu lesen

Sicherheitsanbieter sind insofern ungewöhnlich, als das Produkt mit den weitreichendsten Berechtigungen auf Ihren Systemen läuft und der Vertrag regelt, was der Anbieter mit dem, was er sieht, tun darf. Die oben genannten Vereinbarungen definieren beides. Insbesondere das Material zur Data Governance beantwortet die Frage, die die meisten Sicherheitsfragebögen indirekt stellen: *Was erfasst dieser Anbieter tatsächlich, und wohin gelangen diese Daten?*

Was ist die Cyber Crucible Mutual NDA und wer ist an sie gebunden?

Kurze Antwort: Es handelt sich um eine verbindliche gegenseitige Vertraulichkeitsvereinbarung (Mutual NDA), die jeder Mitarbeiter, Auftragnehmer und Lieferant von Cyber Crucible mit potenziellem Zugriff auf betriebliche Kundendaten oder Managementsysteme **vor dem Onboarding** unterzeichnen muss. Sie ist veröffentlicht unter cybercrucible.com/mutualNDA.

Wer unterzeichnet sie

Alle Personen mit potenziellem Zugriff auf betriebliche Kundendaten oder Managementsysteme werden vor dem Onboarding rechtlich gebunden. Dies umfasst Mitarbeiter, Auftragnehmer und Lieferanten – nicht nur das eigene Personal.

Warum „gegenseitig“ entscheidend ist

Eine einseitige NDA schützt nur den Anbieter. Eine gegenseitige Vereinbarung verpflichtet Cyber Crucible dazu, *Ihre* vertraulichen Informationen zu denselben Bedingungen zu schützen, die das Unternehmen für seine eigenen Informationen erwartet. Für einen Sicherheitsanbieter, dessen Personal möglicherweise betriebliche Details Ihrer Umgebung einsehen kann, ist genau diese Symmetrie entscheidend.

Wie es sich in die übrigen Kontrollen einfügt

Die NDA bildet die vertragliche Ebene einer umfassenderen Risikostrategie gegen Insider-Risiken:

- **Vertraglich** – verbindliche gegenseitige NDA, bevor überhaupt Zugriff gewährt wird.
- **Zugriff** – administrativer Zugriff auf Kunden-Management-Instanzen ist auf überprüftes Personal beschränkt, streng nach dem Need-to-know-Prinzip, nur wenn dies für einen validierten Geschäfts- oder Supportvorgang erforderlich ist.

- **Trennung** – wenn ein Lieferant, Anbieter, Auftragnehmer oder Mitarbeiter ein Sicherheits-, Datenschutz- oder Immaterialgüterrechtsrisiko darstellt, steuert und isoliert Cyber Crucible dieses Risiko aktiv oder trennt sich umgehend von der betreffenden Ressource.

Die NDA begründet die Verpflichtung. Die Zugriffskontrollen begrenzen, wie viel Schaden eine einzelne Person anrichten könnte. Das Trennungsgebot macht beides in der Praxis durchsetzbar.

Was decken die MSA und die EULA ab?

Kurze Antwort: Der Master Services Agreement (MSA) regelt die geschäftliche Beziehung – Leistungen, Pflichten, Haftung und Laufzeit. Die End User License Agreement (EULA) regelt die Nutzung der Software selbst, einschließlich des Lizenzumfangs, der für kompilierten Objektcode gilt und nicht für den Quellcode.

Wichtige Punkte, die Sie vor der Unterzeichnung kennen sollten

- **Lizenzumfang** — die gewährten Rechte gelten für die kompilierte Objektcode-Form der Software. Die Vereinbarung gewährt keine Rechte zum Erhalt oder zur Nutzung des Quellcodes.
- **Keine stillschweigenden Lizenzen** — Cyber Crucible behält sämtliche Rechte, Eigentumsrechte und Ansprüche an den Diensten, der Dokumentation und dem zugehörigen geistigen Eigentum. Es wird nichts stillschweigend gewährt.
- **Implementierungsleistungen** — Konfiguration, Anpassung, Personalschulung oder technischer Support werden in einem Order Form festgelegt und nicht vorausgesetzt.
- **Vertraulichkeit** — beide Parteien können Zugang zu vertraulichen Informationen der jeweils anderen Partei erhalten; diese bleiben jeweils Eigentum der offenlegenden Partei.

Wo Sie es nachlesen können

Die vollständige Vereinbarung ist unter cybercrucible.com/msa-and-eula veröffentlicht. Diese Seite dient nur zur Orientierung und ist kein Ersatz — maßgeblich ist die veröffentlichte Vereinbarung.

Was deckt das Service Level Agreement ab?

Kurze Antwort: Das SLA definiert die Service-Verpflichtungen, die Cyber Crucible gegenüber Kunden eingeht — Verfügbarkeit, Support-Reaktionszeiten und die zugehörigen Bedingungen. Es ist unter cybercrucible.com/service-level-agreement veröffentlicht.

Wie das SLA mit dem Produktdesign zusammenhängt

Erwähnenswert für alle, die eine Bewertung vornehmen: Da die Prävention autonom auf dem Endpunkt erfolgt, typischerweise in unter 200 Millisekunden, hängt der Schutz nicht von der Verfügbarkeit eines Dienstes ab, wie es bei einem Produkt mit Cloud-Analyse der Fall wäre.

Ein Endpunkt, dessen Verwaltungsserver nicht erreichbar ist — oder der bewusst air-gapped betrieben wird — bleibt vollständig geschützt. Bedrohungsbewertung und Prozessunterbrechung erfolgen lokal. Die Verfügbarkeit der Verwaltungsebene wirkt sich auf Berichterstattung und Administration aus, nicht auf die Abwehr.

Das ist ein bedeutsamer Unterschied beim Vergleich von SLAs verschiedener Anbieter. Bei einem cloud-abhängigen Tool kann ein Ausfall der Verwaltungsebene reduzierten oder fehlenden Schutz bedeuten. Hier ist das nicht der Fall.

Wo Sie es nachlesen können

Die vollständige Vereinbarung finden Sie unter cybercrucible.com/service-level-agreement. Verpflichtungen zur Support-Reaktionszeit sowie umgebungsspezifische Bedingungen sollten mit Ihrem Cyber Crucible-Ansprechpartner bestätigt werden.

Wie fülle ich einen Sicherheitsfragebogen oder eine Lieferantenrisikobewertung für Cyber Crucible aus?

Kurze Antwort: Die meisten Fragen werden durch die Datenschutz-Governance-Materialien beantwortet — was erfasst wird, was niemals erfasst wird, wie die Daten bei der Übertragung geschützt werden, wo sie verarbeitet werden und welche Bereitstellungsmodelle verfügbar sind. Für alles, was eine unterzeichnete Dokumentation erfordert, wenden Sie sich bitte an **dpo@cybercrucible.com**.

Die Antworten, die die meisten Fragebögen benötigen

Typische Frage	Wo sie beantwortet wird
Welche Kundendaten erfasst der Anbieter?	*Welche Daten erfasst Cyber Crucible — und welche werden niemals erfasst?*
Werden Daten an Dritte weitergegeben oder verkauft?	*Verkauft oder teilt Cyber Crucible Kundendaten mit Dritten?*
Wie werden Daten bei der Übertragung verschlüsselt?	*Wie werden Cyber-Crucible-Daten bei der Übertragung geschützt?*
Wo werden Daten verarbeitet und gespeichert?	*Wo werden meine Daten verarbeitet, und können sie innerhalb meines Landes verbleiben?*
Unterauftragsverarbeiter und Kontrollen der Lieferkette?	*Wie verwaltet Cyber Crucible Risiken in der Lieferkette und durch Insider?*
Komponenten von Drittanbietern oder ausländischer Code?	*Bindet Cyber Crucible Bibliotheken von Drittanbietern oder ausländischen Code ein?*
Rolle als Verantwortlicher oder Auftragsverarbeiter?	*Ist Cyber Crucible ein Verantwortlicher oder ein Auftragsverarbeiter?*
Mechanismus für grenzüberschreitende Übertragungen?	*Wie werden grenzüberschreitende Datenübertragungen gehandhabt?*

Zwei Antworten, die Prüfer häufig überraschen

Zu Zertifizierungen: Das Sicherheitsprogramm von Cyber Crucible ist an anerkannten Branchenstandards ausgerichtet, verfügt jedoch **derzeit nicht über eine ISO-27001- oder SOC-2-Zertifizierung**. Wenn Ihr Prozess zertifizierte Nachweise erfordert, sprechen Sie dies frühzeitig und nicht erst spät an.

Zur Offenlegung von Daten: Da Verschlüsselungsschlüssel, Zugangsdaten und Kundendateien niemals erfasst werden, gibt es in diesen Kategorien nichts, das gegenüber irgendeiner Partei — auch nicht im Rahmen rechtlicher Verfahren — offengelegt werden könnte. Mehrere Fragebogenpunkte zu Offenlegung, Aufbewahrung und Löschung werden durch das Fehlen der Erfassung beantwortet, nicht durch eine Kontrollmaßnahme.

Alles, was nicht abgedeckt ist

Wenden Sie sich mit der konkreten Anforderung, Ihrer Rechtsordnung und dem von Ihnen bewerteten Bereitstellungsmodell an **dpo@cybercrucible.com**.