Documents juridiques et de confiance

Où trouver les accords et la documentation de confiance de Cyber Crucible — accord de confidentialité mutuel (NDA), contrat-cadre de services (MSA) et contrat de licence utilisateur final (EULA), contrat de niveau de service, accords de traitement des données et preuves de conformité.

Où puis-je trouver les documents juridiques et de confiance de Cyber Crucible ?

Réponse courte : Les accords publics sont publiés sur cybercrucible.com — l'Accord de non-divulgation mutuel, le MSA et le CLUF, l'Accord de niveau de service, la Politique de confidentialité et les Conditions d'utilisation. La documentation de conformité fournie sur demande — Clauses contractuelles types, Évaluation des risques de transfert, et Accords de traitement des données — provient de **dpo@cybercrucible.com**.

Disponible publiquement

Document	Emplacement
Accord de non-divulgation mutuel	cybercrucible.com/mutualNDA
Accord-cadre de services et CLUF	cybercrucible.com/msa-and-eula
Accord de niveau de service	cybercrucible.com/service-level-agreement
Politique de confidentialité	cybercrucible.com/privacy-policy
Conditions d'utilisation	cybercrucible.com/terms-of-service

Fourni sur demande

Contactez **dpo@cybercrucible.com** pour obtenir :

- Les Clauses contractuelles types, y compris les clauses préapprouvées par la SDAIA pour les transferts vers l'Arabie saoudite
- L'Évaluation des risques de transfert
- L'Accord de traitement des données
- La documentation relative à la gouvernance des données et à la politique de partage

Ces documents sont fournis sous réserve de mesures de confidentialité raisonnables.

Pourquoi il est utile de les consulter avant tout achat

Les fournisseurs de solutions de sécurité présentent une particularité : le produit fonctionne avec les privilèges les plus élevés sur vos systèmes, et le contrat régit ce que le fournisseur est autorisé à faire avec ce qu'il observe. Les accords mentionnés ci-dessus définissent ces deux aspects. La documentation relative à la gouvernance des données répond en particulier à la question que la plupart des questionnaires de sécurité posent de manière indirecte : *que collecte réellement ce fournisseur, et où ces données vont-elles ?*

Qu'est-ce que l'accord de confidentialité mutuel (NDA) de Cyber Crucible, et qui y est soumis ?

Réponse courte : Il s'agit d'un accord de confidentialité mutuel contraignant que chaque employé, contractant et fournisseur de Cyber Crucible susceptible d'accéder aux données opérationnelles ou aux systèmes de gestion des clients doit signer **avant son intégration**. Il est publié à l'adresse cybercrucible.com/mutualNDA.

Qui le signe

Tout le personnel susceptible d'accéder aux données opérationnelles ou aux systèmes de gestion des clients est juridiquement engagé avant son intégration. Cela inclut les employés, les contractants et les fournisseurs — pas uniquement le personnel interne.

Pourquoi le caractère « mutuel » importe

Un accord de confidentialité à sens unique ne protège que le fournisseur. Un accord mutuel engage Cyber Crucible à protéger *vos* informations confidentielles selon les mêmes conditions que celles qu'il attend pour les siennes. Pour un fournisseur de sécurité dont le personnel peut avoir accès à des détails opérationnels sur votre environnement, cette symétrie est essentielle.

Comment cela s'inscrit avec les autres contrôles

Le NDA constitue la couche contractuelle d'une posture plus large de gestion du risque interne :

- **Contractuel** — accord de confidentialité mutuel contraignant avant tout octroi d'accès.

- **Accès** — accès administratif aux instances de gestion des clients limité au personnel habilité, strictement selon le principe du besoin d'en connaître, uniquement lorsque cela est requis pour une opération commerciale ou de support validée.
- **Fin de collaboration** — si un fournisseur, sous-traitant, contractant ou employé présente un risque en matière de sécurité, de confidentialité ou de propriété intellectuelle, Cyber Crucible gère et isole activement ce risque ou met fin immédiatement à la collaboration avec la ressource concernée.

Le NDA établit l'obligation. Les contrôles d'accès limitent l'ampleur des abus possibles par une seule personne. L'obligation de mettre fin à la collaboration est ce qui rend les deux applicables en pratique.

Que couvrent le MSA et le CLUF ?

Réponse courte : le Master Services Agreement (contrat-cadre de services) régit la relation commerciale — services, obligations, responsabilité et durée. Le Contrat de Licence Utilisateur Final (CLUF) régit l'utilisation du logiciel proprement dit, y compris le périmètre de la licence, laquelle s'applique au code objet compilé et non au code source.

Points clés à connaître avant de signer

- **Périmètre de la licence** — les droits accordés s'appliquent à la forme du logiciel sous code objet compilé. L'accord n'accorde aucun droit d'obtenir ou d'utiliser le code source.
- **Absence de licence implicite** — Cyber Crucible conserve l'ensemble des droits, titres et intérêts relatifs aux services, à la documentation et à la propriété intellectuelle associée. Aucun droit n'est accordé de manière implicite.
- **Services de mise en œuvre** — la configuration, la personnalisation, la formation du personnel ou le support technique sont définis dans un bon de commande (Order Form) et ne sont pas présumés.
- **Confidentialité** — chaque partie peut avoir accès aux informations confidentielles de l'autre ; celles-ci demeurent la propriété de la partie qui les divulgue.

Où le consulter

L'accord complet est publié à l'adresse cybercrucible.com/msa-and-eula. Cette page constitue un résumé à titre indicatif, et non un substitut — c'est l'accord publié qui fait foi.

Que couvre l'Accord de niveau de service ?

Réponse courte : Le SLA définit les engagements de service que Cyber Crucible prend envers ses clients — disponibilité, réactivité du support, et les conditions associées. Il est publié à l'adresse cybercrucible.com/service-level-agreement.

Comment le SLA s'articule avec la conception du produit

Point important pour toute personne en phase d'évaluation : la prévention s'effectue de manière autonome sur le poste de travail, généralement en moins de 200 millisecondes, la protection ne dépend donc pas de la disponibilité d'un service comme c'est le cas pour un produit reposant sur une analyse cloud.

Un poste dont le serveur de gestion est inaccessible — ou qui est volontairement isolé du réseau (air-gapped) — reste entièrement protégé. L'évaluation des menaces et l'interruption des processus s'effectuent localement. La disponibilité du plan de gestion affecte le reporting et l'administration, pas la défense.

Il s'agit d'une distinction importante lors de la comparaison des SLA entre fournisseurs. Pour un outil dépendant du cloud, une indisponibilité du plan de gestion peut signifier une protection réduite ou absente. Ici, ce n'est pas le cas.

Où le consulter

L'accord complet est disponible à l'adresse cybercrucible.com/service-level-agreement. Les engagements en matière de réactivité du support et toute condition spécifique à un environnement donné doivent être confirmés auprès de votre représentant Cyber Crucible.

Comment remplir un questionnaire de sécurité ou une évaluation des risques fournisseurs pour Cyber Crucible ?

Réponse courte : La plupart des questions trouvent leur réponse dans la documentation relative à la gouvernance des données — ce qui est collecté, ce qui n'est jamais collecté, comment les données sont protégées en transit, où elles sont traitées, et quels modèles de déploiement sont disponibles. Pour tout ce qui nécessite une documentation signée, contactez **dpo@cybercrucible.com**.

Les réponses dont la plupart des questionnaires ont besoin

Question type	Où trouver la réponse
Quelles données clients le fournisseur collecte-t-il ?	*Quelles données Cyber Crucible collecte-t-il — et lesquelles ne collecte-t-il jamais ?*
Les données sont-elles partagées avec des tiers ou vendues à des tiers ?	*Cyber Crucible vend-il ou partage-t-il les données clients avec des tiers ?*
Comment les données sont-elles chiffrées en transit ?	*Comment les données de Cyber Crucible sont-elles protégées en transit ?*
Où les données sont-elles traitées et stockées ?	*Où mes données sont-elles traitées, et peuvent-elles rester dans mon pays ?*
Sous-traitants et contrôles de la chaîne d'approvisionnement ?	*Comment Cyber Crucible gère-t-il les risques liés à la chaîne d'approvisionnement et aux menaces internes ?*
Composants de code tiers ou étrangers ?	*Cyber Crucible intègre-t-il des bibliothèques tierces ou du code étranger ?*
Rôle de responsable ou de sous-traitant ?	*Cyber Crucible est-il un responsable du traitement ou un sous-traitant ?*

Question type	Où trouver la réponse
Mécanisme de transfert transfrontalier ?	*Comment les transferts de données transfrontaliers sont-ils gérés ?*

Deux réponses qui surprennent souvent les évaluateurs

Concernant les certifications : le programme de sécurité de Cyber Crucible s'aligne sur des référentiels reconnus du secteur, mais **ne détient actuellement pas de certification ISO 27001 ou SOC 2**. Si votre processus exige des preuves certifiées, signalez-le dès le départ plutôt qu'en fin de parcours.

Concernant la divulgation des données : étant donné que les clés de chiffrement, les identifiants et les fichiers clients ne sont jamais collectés, il n'y a rien à divulguer dans ces catégories à quelque partie que ce soit — y compris dans le cadre d'une procédure judiciaire. Plusieurs éléments des questionnaires portant sur la divulgation, la conservation et la suppression trouvent leur réponse dans l'absence de collecte plutôt que dans un contrôle.

Ce qui n'est pas couvert

Contactez **dpo@cybercrucible.com** en précisant l'exigence spécifique, votre juridiction, et le modèle de déploiement que vous évaluez.