

C2I INFO

Conditions Particulières – Cybersécurité

Version 1.3 – 29 septembre 2026

C2i info, SARL au capital de 5 000 €, dont le siège social est situé 34B rue du Général Franiatte, 57950 Montigny-lès-Metz, immatriculée au RCS de Metz sous le numéro 795 003 490, TVA intracommunautaire FR 90 795 003 490 –
Téléphone : 03 87 51 26 27 – Courriel : contact@c2i-info.net – Site : <https://c2i-info.net>

Sommaire

- Article 1 – Objet et documents applicables
- Article 2 – Principes
- Article 3 – Protection des postes et serveurs (EDR)
- Article 4 – Sécurité de la messagerie et de Microsoft 365
- Article 5 – Sensibilisation et simulations d'hameçonnage
- Article 6 – Gestionnaire de mots de passe
- Article 7 – Audits et diagnostics de sécurité
- Article 8 – Tests d'intrusion
- Article 9 – Assistance en cas d'incident de sécurité
- Article 10 – Données personnelles
- Article 11 – Responsabilité
- Article 12 – Fin des Services Cyber

Article 1 – Objet et documents applicables

Les présentes Conditions Particulières définissent les conditions dans lesquelles C2i info (le « Prestataire ») fournit au Client, selon la Commande, les services de cybersécurité suivants (les « Services Cyber ») :

- la protection des postes, serveurs et terminaux mobiles par des solutions de détection et de réponse (EDR), éventuellement associées à un centre opérationnel de sécurité (SOC) ;
- la protection de la messagerie contre le spam et l'hameçonnage, par les fonctions de Microsoft 365 ou par une solution spécialisée d'un éditeur tiers ;
- le paramétrage et l'administration des fonctions de sécurité de Microsoft 365 : Microsoft Defender, gestion des terminaux (Intune), protection des informations (Purview) et contrôle des accès (Entra ID) ;
- la sensibilisation des Utilisateurs et les campagnes de simulation d'hameçonnage ;
- la fourniture d'un gestionnaire de mots de passe ;
- les audits et diagnostics de sécurité ;
- l'assistance en cas d'incident de sécurité ;
- les tests d'intrusion, lorsque le Prestataire les propose.

Elles complètent les Conditions Générales de Vente et de Services – Informatique (les « CGVS »), dont les termes définis s'appliquent aux présentes. En cas de contradiction, les présentes Conditions Particulières prévalent pour ce qui concerne les Services Cyber. Les licences Microsoft sur lesquelles reposent certains Services Cyber relèvent en outre des Conditions Particulières Microsoft 365 et Cloud.

Article 2 – Principes

Les Services Cyber réduisent le risque d'attaque informatique et en limitent les conséquences ; ils ne peuvent le supprimer. Aucune solution ne détecte ni ne bloque la totalité des menaces, qui évoluent en permanence. Le Prestataire est tenu à une obligation de moyens.

Le label ExpertCyber dont bénéficie le Prestataire atteste de son niveau d'expertise et de ses pratiques ; il ne constitue pas une garantie de résultat quant à la sécurité du système d'information du Client.

La sécurité du système d'information repose aussi sur le Client : mises à jour, sauvegardes, gestion des accès, vigilance des Utilisateurs. Le Client s'engage à mettre en œuvre les recommandations écrites du Prestataire ; s'il décide de ne pas les suivre, il en assume les conséquences conformément à l'article 9 des CGVS.

Article 3 – Protection des postes et serveurs (EDR)

3.1 Solutions

Le Prestataire fournit, selon la Commande, une licence de solution de détection et de réponse d'un éditeur tiers, ou met en œuvre celle incluse dans les licences Microsoft 365 du Client (Microsoft Defender), pour chaque poste, serveur ou terminal mobile du Périmètre. Chaque solution comprend les fonctions décrites par son éditeur (antivirus nouvelle génération, détection comportementale, isolement des machines compromises, contrôle des périphériques, selon l'offre souscrite).

Le Client dispose d'un droit d'utilisation non exclusif, non cessible et limité à la durée de l'abonnement, sur les seuls équipements couverts. Il s'engage à respecter les conditions de licence de l'éditeur, que le Prestataire lui communique sur demande, et s'interdit notamment de désactiver l'agent de protection, d'en contourner le fonctionnement ou de donner accès à la console à des tiers non autorisés.

3.2 Répartition des rôles

Le Prestataire installe l'agent de protection, configure les politiques de sécurité et gère les licences.

Offres sans SOC : le Prestataire analyse les alertes et met en œuvre les actions de remédiation pendant les Heures Ouvrées, selon les délais de l'Annexe A des CGVS. Les alertes survenant en dehors de ces heures sont traitées automatiquement par la solution selon les politiques configurées, puis analysées à l'ouverture de la plage suivante.

Offres avec SOC : les alertes sont analysées par le centre opérationnel de sécurité associé à la solution, y compris en dehors des Heures Ouvrées pour les alertes critiques. Le SOC peut déclencher des actions de réponse à distance. Le Prestataire réalise ensuite, pendant les Heures Ouvrées, les interventions nécessaires sur les équipements (correctifs, remise en service).

3.3 Actions automatiques

Le Client autorise la solution, le SOC et le Prestataire à prendre toute mesure de protection immédiate en cas de menace, notamment l'isolement d'un poste ou d'un serveur du réseau, l'arrêt d'un processus ou la mise en quarantaine d'un fichier. Ces mesures peuvent interrompre temporairement l'activité de l'équipement concerné. Elles peuvent aussi résulter d'une fausse alerte ; le Prestataire rétablit alors le fonctionnement normal dans les meilleurs délais. Ces interruptions n'engagent pas la responsabilité du Prestataire.

3.4 Obligations du Client

- déclarer au Prestataire tout nouvel équipement à protéger et ne pas désinstaller l'agent d'un équipement du Périmètre ;
- maintenir ses systèmes d'exploitation dans une version supportée par leur éditeur et par la solution de protection ;
- ne pas installer de logiciel de sécurité concurrent susceptible de perturber la solution, sans l'accord du Prestataire.

3.5 Ajustement du nombre de licences

Le Prestataire contrôle le nombre d'équipements protégés. Lorsque ce nombre dépasse le nombre de licences souscrites, les licences supplémentaires sont ajoutées à l'abonnement à compter du mois suivant et facturées au Client, qui en est informé. Une réduction du nombre de licences n'est possible qu'à l'échéance de l'engagement souscrit auprès de l'éditeur.

3.6 Conformité réglementaire

Le Client déclare que ni lui ni ses Utilisateurs ne font l'objet de sanctions économiques internationales, qu'il n'utilise pas les solutions dans un pays soumis à embargo ni à des fins interdites par les réglementations sur le contrôle des exportations de l'Union européenne ou des États-Unis. Il coopère aux vérifications demandées par l'éditeur et accepte que l'éditeur ou le Prestataire suspende l'accès aux solutions en cas de manquement à ces règles.

Article 4 – Sécurité de la messagerie et de Microsoft 365

Lorsque la Commande le prévoit, le Prestataire paramètre et administre les fonctions de sécurité incluses dans les licences Microsoft 365 du Client. Les règles définies ont une incidence directe sur l'activité des Utilisateurs ; elles sont mises en place après validation par le Client et peuvent être ajustées à sa demande.

4.1 Protection de la messagerie

La protection de la messagerie repose, selon la Commande, sur les fonctions de filtrage de Microsoft 365 et, le cas échéant, sur une solution spécialisée d'un éditeur tiers connectée aux boîtes aux lettres du Client, qui analyse les courriels reçus et intègre les signalements des Utilisateurs.

Le Client autorise la solution et le Prestataire à retirer automatiquement un courriel identifié comme malveillant de l'ensemble des boîtes aux lettres concernées, y compris après sa distribution, et à le placer en quarantaine.

Le filtrage des courriels réduit fortement les messages indésirables et frauduleux sans pouvoir tous les arrêter. Il peut aussi placer par erreur des messages légitimes en quarantaine. Le Client et ses Utilisateurs consultent régulièrement la quarantaine et signalent au Prestataire les erreurs de filtrage. Le Prestataire n'est pas responsable d'un message légitime bloqué ni d'un message frauduleux non détecté malgré une configuration conforme.

4.2 Gestion des terminaux (Intune)

La gestion des terminaux permet d'appliquer des règles de sécurité aux ordinateurs, téléphones et tablettes des Utilisateurs et, en cas de perte ou de vol, de les verrouiller ou d'en effacer le contenu à distance.

Un effacement à distance est irréversible. Le Prestataire ne le réalise que sur demande écrite du Client, émanant d'une personne habilitée, ou, en cas d'urgence, sur demande orale confirmée par écrit dans les meilleurs délais. Sur les appareils personnels des Utilisateurs, seules les données et applications professionnelles sont gérées et effacées. Le Client informe ses Utilisateurs de ces règles, notamment dans sa charte informatique.

4.3 Protection des informations (Purview)

Les règles de classification, de prévention des fuites de données et de conservation sont définies par le Client, qui connaît la nature et les obligations légales de conservation de ses données. Le Prestataire les paramètre selon ses instructions. Une règle de conservation peut entraîner la suppression automatique de données à l'expiration de la durée fixée ; une règle de prévention des fuites peut bloquer un envoi légitime. Le Client valide ces règles avant leur activation.

4.4 Contrôle des accès (Entra ID)

Les règles d'authentification multifacteur et d'accès conditionnel peuvent bloquer la connexion d'un Utilisateur qui ne les respecte pas. Le Client conserve au moins un compte d'administration d'urgence, exclu de ces règles et protégé, afin de ne jamais perdre l'accès à son environnement.

Article 5 – Sensibilisation et simulations d'hameçonnage

Le Prestataire met à disposition du Client une plateforme de sensibilisation comprenant des modules de formation en ligne et des campagnes de simulation d'hameçonnage. Ces campagnes consistent à envoyer aux Utilisateurs de faux courriels frauduleux afin de mesurer et d'améliorer leur vigilance.

Avant toute campagne, le Client :

- autorise par écrit, par l'intermédiaire de son représentant légal ou d'une personne habilitée, la réalisation de la campagne et son périmètre ;
- informe ses salariés, de manière générale, que des simulations d'hameçonnage peuvent être organisées à des fins de sensibilisation, sans nécessairement en préciser les dates, et consulte le cas échéant ses représentants du personnel ;
- fournit la liste des Utilisateurs concernés et autorise les paramétrages techniques nécessaires à la bonne réception des courriels de simulation.

Le Client s'engage à utiliser les résultats des campagnes à des fins de sensibilisation et de formation, et non pour sanctionner individuellement ses salariés. Le Prestataire s'abstient d'utiliser dans les simulations des procédés susceptibles de porter atteinte à la dignité des Utilisateurs ou de causer une alarme excessive (par exemple un faux message de licenciement ou de santé).

Article 6 – Gestionnaire de mots de passe

Le gestionnaire de mots de passe fourni repose sur un chiffrement dit « à connaissance nulle » : ni l'éditeur ni le Prestataire n'ont accès au contenu des coffres des Utilisateurs. Chaque Utilisateur est responsable de la confidentialité de son mot de passe principal. Un mot de passe principal perdu peut rendre le contenu du coffre définitivement inaccessible, sauf si une procédure de récupération a été configurée par l'administrateur du Client.

Article 7 – Audits et diagnostics de sécurité

Les audits et diagnostics sont réalisés selon la méthode et le périmètre décrits dans la Commande. Ils reflètent l'état du système d'information à la date de leur réalisation, sur la base des éléments accessibles et des informations fournies par le Client. Ils ne constituent pas une garantie d'absence de vulnérabilité.

Le rapport remis au Client contient des informations sensibles sur sa sécurité. Le Client le conserve de manière confidentielle et ne le diffuse qu'aux personnes qui ont besoin d'en connaître. La mise en œuvre des recommandations relève de la décision du Client et fait l'objet, le cas échéant, d'une Commande distincte.

Article 8 – Tests d'intrusion

Lorsqu'ils sont proposés, les tests d'intrusion ne sont réalisés qu'après signature par le représentant légal du Client d'une autorisation écrite précisant le périmètre (adresses, applications, équipements), les dates et horaires, les techniques autorisées et les personnes à contacter. Toute action hors de ce périmètre est exclue. Cette autorisation est indispensable, l'accès frauduleux à un système d'information étant pénalement sanctionné (article 323-1 du Code pénal).

Le Client garantit qu'il est titulaire des systèmes testés ou qu'il a obtenu l'accord de leurs hébergeurs ou fournisseurs lorsque leurs conditions l'exigent. Il est informé que les tests peuvent provoquer des ralentissements ou des interruptions, et réalise au préalable une sauvegarde de ses données.

Article 9 – Assistance en cas d'incident de sécurité

En cas d'incident de sécurité, notamment d'attaque par rançongiciel, le Prestataire intervient pour contenir l'incident, en analyser l'origine dans la mesure de ses moyens et accompagner la remise en service du système d'information. Sauf si elle est comprise dans le Service souscrit, cette assistance est facturée au temps passé selon le tarif en vigueur. Le Prestataire peut orienter le Client vers un prestataire spécialisé en réponse à incident lorsque la situation le requiert.

Le rétablissement des données dépend de l'existence et de l'intégrité des sauvegardes. Le Prestataire ne garantit pas la récupération de l'ensemble des données.

Le Client reste responsable de ses démarches, notamment la notification à la CNIL dans les 72 heures en cas de violation de données personnelles, la déclaration à son assureur et le dépôt de plainte. Le Prestataire l'assiste dans la préparation de ces démarches et préserve, dans la mesure du possible, les éléments de preuve.

Conformément aux recommandations des autorités, le Prestataire ne négocie pas et ne paie pas de rançon, et déconseille au Client de le faire.

Article 10 – Données personnelles

Les solutions de protection collectent des données techniques sur les équipements (processus, fichiers, connexions, noms d'utilisateur) afin de détecter les menaces. La plateforme de sensibilisation traite les noms, adresses électroniques et résultats des Utilisateurs. Ces traitements sont réalisés pour le compte du Client, le Prestataire et les éditeurs agissant en qualité de sous-traitants dans les conditions de l'Annexe B des CGVS. Les données traitées par les fonctions de sécurité de Microsoft 365 le sont par Microsoft dans les conditions de son accord sur la protection des données, intégré au Microsoft Customer Agreement.

Il appartient au Client d'informer ses Utilisateurs de la mise en œuvre de ces outils, notamment par sa charte informatique.

Article 11 – Responsabilité

Outre les exclusions prévues par les CGVS, le Prestataire n'est pas responsable :

- d'une attaque que les solutions n'ont pas détectée ou bloquée malgré une configuration conforme ;
- des interruptions résultant des mesures de protection automatiques ou d'une fausse alerte ;
- des conséquences d'un défaut de mise à jour, d'un équipement non protégé ou non déclaré, d'un agent désactivé ou d'une recommandation non suivie ;
- des défaillances des éditeurs et de leurs plateformes.

Il reste responsable, dans les limites des CGVS, de la bonne installation, de la bonne configuration des solutions et du traitement des alertes qui lui incombent.

Article 12 – Fin des Services Cyber

Les licences sont souscrites pour la durée d'engagement indiquée dans la Commande et restent dues jusqu'à leur échéance conformément à l'article 21 des CGVS. À la fin d'un Service, le Prestataire désinstalle ou désactive les agents à la demande du Client ; à défaut, ceux-ci cessent de protéger les équipements. Si un éditeur met fin à l'autorisation de revente du Prestataire, celui-ci en informe le Client et lui propose une solution équivalente.