Conditions générales de vente et prestations de services aux entreprises et professionnels

ARTICLE 1 : CHAMP D'APPLICATION

Les présentes Conditions Générales de Vente s'appliquent à toutes les prestations de services et ventes de matériels conclues par la Société TRILOG, ci-après dénommée "le prestataire" auprès des clients professionnels, ci-après dénommés "le client", quelle que soient les clauses pouvant figurer sur les documents du Client, et notamment ses conditions générales d'achat, sur lesquelles les présentes Conditions Générales de Vente prévalent, et concernent :

- La vente de matériel informatique (réseau, PC, écran, …) et logiciels,
- la location de matériels informatiques avec option d'achat,
- La vente de prestations de services de maintenance informatique et de dépannage, notamment par hotline,
- la formation dans le domaine informatique,
- La sauvegarde externalisée de données.

Elles ne s'appliquent pas :

- aux prestations portant sur les matériels d'alimentation statique qui font l'objet de conditions générales spécifiques
- aux contrats de location financières, auxquels seules sont applicables les conditions générales de location de l'organisme de financement.

Conformément à la réglementation en vigueur, ces Conditions Générales sont systématiquement communiquées à tout Client qui en fait la demande, pour lui permettre de passer commande auprès du Prestataire.

Les présentes Conditions Générales de Vente peuvent éventuellement être complétées et/ou modifiées par des clauses particulières, figurant notamment dans le devis, l'offre acceptée et/ ou le contrat convenu avec le Client.

Les Conditions Générales sont consultables en permanence sur le site Internet de la société TRILOG. Elles sont susceptibles d'être modifiées à tout moment et sans préavis. Les Conditions Générales applicables sont celles en vigueur sur le site à la date de la demande du Client (date du devis ou date de la commande en cas de prestations sans devis). Pour les contrats à exécution successive, les mises à jour des conditions générales de vente sont opposables au client dès lors qu'elles ont été portées à sa connaissance par tout moyen écrit, notamment lors de la conclusion d'un nouveau contrat.

Dès lors qu'il adresse une commande à TRILOG le Client déclare avoir la pleine capacité juridique lui permettant de s'engager ou tous pouvoirs lui permettant d'engager la société, et déclare adhérer sans restriction ni réserve aux présentes Conditions Générales.

ARTICLE 2 : COMMANDE

Les ventes de matériel, logiciels et prestations ne sont parfaites qu'après acceptation expresse et par écrit de la commande du Client par le Prestataire, matérialisée par l'acceptation par le Client du devis définitif ou de l'offre définitive émis(e) par TRILOG.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Les éventuelles modifications de la commande demandées par le Client ne seront prises en compte, dans la limite des possibilités du Prestataire, que si elles sont notifiées par écrit, quinze (15) jours au moins avant la date prévue pour la fourniture des prestations de services commandées, après signature par le Client d'un nouveau devis spécifique et ajustement éventuel du prix.

En cas d'annulation de la commande par le Client après son acceptation par le Prestataire, pour quelque raison que ce soit hormis la force majeure, l'acompte versé à la commande sera de plein droit acquis au Prestataire et ne pourra donner lieu à un quelconque remboursement. A défaut d'acompte, une somme correspondant à 30 % du montant TTC de la facture totale sera acquise au Prestataire, à titre de dommages et intérêts, en réparation du préjudice ainsi subi.

ARTICLE 3 – DUREE DES CONTRATS

Les contrats de location de matériels informatiques sont conclus pour la durée indiquée au contrat de location conclu avec le fournisseur et l'organisme de financement,

Les contrats de vente de prestations de services de maintenance et de dépannage de matériel informatique, notamment par hotline prennent effet le jour de l'installation du matériel commandé ou de réalisation de l'audit du matériel conservé par le Client pour une durée d'un (1) an renouvelable par tacite reconduction d'année en année, sauf dénonciation du contrat par l'une ou l'autre des parties trois (3) mois avant la date d'échéance par lettre recommandée avec accusé de réception.

Les contrats de sauvegarde externalisée de données Kiwi Backup prennent effet le jour de l'installation du logiciel de sauvegarde de données pour une durée une durée initiale de (douze) 12 mois à compter de la date de la signature du Bon de commande. Le Contrat se renouvellera ensuite par période successive d'un an, dans les mêmes termes.

Les autres contrats de sauvegarde externalisée de données prennent effet le jour de l'installation du logiciel de sauvegarde de données pour une durée indéterminée, chaque partie pourra y mettre fin à tout moment avec un préavis de DEUX (2) mois par lettre recommandée avec accusé de réception.

Les contrats de suivi et de télémaintenance de logiciels, autres que ceux relatifs à la sauvegarde de données, sont conclus pour une durée indéterminée et sont résiliables par l'une ou l'autre des parties par lettre recommandée avec accusé de réception moyennant un préavis de six (6) mois.

ARTICLE 4 - TARIFS

Les produits et services proposés par TRILOG sont fournis aux tarifs en vigueur au jour de la passation de la commande, selon le devis préalablement établi par le Prestataire et accepté par le Client.

Les tarifs s'entendent nets et HT.

Le prix de l'abonnement au Service de sauvegarde externalisée souscrit est forfaitaire et dépend du volume de données sélectionné. Les éléments de calcul du tarif définis au moment de la souscription sont : un volume de données et le prix correspondant au palier. Ce prix sera réévalué périodiquement en fonction de la grille tarifaire en vigueur si le volume de données vient à dépasser la limite en place. Le prix est indiqué en euros hors taxe, sans frais complémentaire. La TVA applicable est celle en vigueur au jour de la facturation.

Le Client sera informé par courriel de ces dépassements de volume et le nouveau tarif s'appliquera sans signature d'un avenant au Contrat initial.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Sont exclues de la redevance mensuelle de sauvegarde et donnent lieu à facturation séparée les prestations suivantes :

. les frais de déplacement et plus généralement toutes prestations n'entrant pas dans l'offre initiale de TRILOG ;
. le coût des télécommunications qui reste entièrement à la charge du Client.

ARTICLE 5 – MODALITES ET DELAIS DE PAIEMENT

Une facture est établie par le Prestataire et remise au Client selon les conditions prévues au devis et/ ou sur l'offre acceptée par le Client.

S'agissant des ventes de matériels, un acompte correspondant à 30 % du prix total des produits commandés est exigé lors de la passation de la commande. Le solde du prix est payable au comptant, au jour de la livraison des matériels. Le Prestataire ne sera pas tenu de procéder à la livraison des matériels si le Client ne lui en paye pas le prix dans les conditions et selon les modalités ci-dessus indiquées.

En cas de retard de paiement des sommes dues par le Client, des pénalités de retard calculées sur la base de trois fois le taux d'intérêt légal, seront automatiquement et de plein droit acquises au Prestataire, sans formalités aucune ni mise en demeure préalable.

En cas de non-respect des conditions de paiement figurant ci-dessus, le Prestataire se réserve en outre le droit de suspendre ou d'annuler la livraison des commandes en cours ou la fourniture des prestations et de diminuer ou d'annuler les éventuelles remises accordées au Client.
En outre, le Prestataire se réserve la faculté de saisir le Tribunal compétent afin que celui-ci fasse cesser cette inexécution sous astreinte journalière par jour de retard.

Aucun escompte ne sera pratiqué pour paiement comptant, ou dans un délai inférieur à celui figurant aux présentes Conditions Générales de Vente, ou sur la facture émise par le Prestataire.

ARTICLE 6 - CLAUSE DE RESERVE DE PROPRIETE

Le transfert de propriété des matériels vendus par le Prestataire est suspendu jusqu'à complet paiement du prix de ceux-ci par le Client, en principal et accessoires, même en cas d'octroi de délai de paiement. Toute clause contraire notamment insérée dans les conditions générales d'achat, est réputée non écrite.

En cas d'ouverture d'une procédure de redressement judiciaire ou de liquidation de biens, les commandes en cours seront automatiquement annulées, et le Prestataire se réserve le droit de revendiquer les biens vendus non réglés.

La présente clause n'empêche pas que les risques des biens vendus soient transférés au Client dès leur livraison à celui-ci.

A compter de la livraison, le Client est constitué dépositaire et gardien des biens vendus et doit les assurer.

Dans le cas de non-paiement, et à moins que le Prestataire ne préfère demander l'exécution pleine et entière de la vente, ce dernier se réserve le droit de résilier la vente après mise-en-demeure et de revendiquer les matériels livrés, les frais de retour restant à la charge du Client et les versements effectués étant acquis au Prestataire à titre de clause pénale.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

ARTICLE 7 – MODALITES DE LIVRAISON DES MATERIELS ET DE FOURNITURE DES PRESTATIONS

7.1 – Délais

Les délais de livraison des matériels et/ou d'exécution des prestations sont communiqués à titre indicatif par le Prestataire après acceptation du devis par le Client.

Ces délais ne constituent pas des délais de rigueur et le Prestataire ne pourra voir sa responsabilité engagée à l'égard du Client en cas de retard de livraison ou d'exécution. Tout retard de livraison ou d'exécution ne peut donner lieu à aucune pénalité ou indemnité, ni motiver l'annulation de la commande ou la résiliation de la vente.

La responsabilité du Prestataire ne pourra en aucun cas être engagée en cas de retard ou de suspension de la livraison ou de l'exécution de la prestation imputable au Client, notamment en cas de non-respect des règles de paiement, ou en cas de force majeure.

7.2 - Livraison des matériels

La livraison sera effectuée au lieu indiqué dans le devis. Les matériels sont réputés livrés dès leur mise à disposition du Client dans les locaux du Prestataire, les matériels voyageant aux risques et périls du Client et à ses frais exclusifs.

Le Client est tenu de vérifier l'état apparent des biens vendus lors de la livraison en présence du livreur. A défaut de réserves expressément formulées par écrit par le Client sur le bon de livraison, les produits délivrés par le Prestataire seront réputés conformes en quantité et qualité à la commande.

Sans préjudice des dispositions à prendre par le Client lors de la livraison, toute réclamation, quelle qu'en soit la nature, portant sur les matériels livrés ne sera admise par le Prestataire que si elle est effectuée par écrit, en lettre recommandée avec AR, dans les trois jours de la réception des biens. Il appartient alors au Client de fournir toutes les justifications quant à la réalité des vices ou des anomalies constatés.

Aucun retour de bien vendu ne pourra être effectué par le Client sans l'accord exprès et préalable du Prestataire.

Le retour s'effectuera par remise à notre livreur au moment de la livraison ou à l'occasion d'une livraison ultérieure, à défaut par le Client à ses frais. Les contestations relatives aux biens intransportables doivent faire l'objet d'une mention par notre livreur sur le bon de livraison.

Lorsqu'après contrôle un vice est effectivement constaté par le Prestataire, le Client ne pourra demander au Prestataire que le remplacement des pièces non-conformes à nos frais, sans pouvoir prétendre à une quelconque indemnité ou à la résolution de la commande.

La réclamation effectuée par le Client dans les conditions et selon les modalités décrites par le présent article ne suspend pas le paiement par le Client des matériels concernés.

7.3 – Fourniture des prestations

Le contenu, les modalités et les conditions d'exécution des prestations de services seront détaillées dans le devis établi par TRILOG et accepté par le Client préalablement à toute intervention.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

A défaut de réserves ou réclamations expressément émises par le Client lors de la réception des prestations, celles-ci seront réputées conformes à la commande, en quantité et qualité.

Le Client disposera d'un délai de huit (8) jours à compter de la fourniture des prestations pour émettre, par écrit, de telles réserves ou réclamations, avec tous les justificatifs y afférents, auprès du Prestataire. Aucune réclamation ne pourra être valablement acceptée en cas de non-respect de ces formalités et délais par le Client.

Le Prestataire rectifiera dans les plus brefs délais et à ses frais, les prestations fournies dont le défaut de conformité aura été dûment prouvé par le Client.

7.4 Interventions techniques

Le Prestataire peut être amené à intervenir techniquement sur les serveurs pour fournir les prestations commandées, mettre fin à un dysfonctionnement technique ou procéder à une opération de maintenance. Les prestations d'assistance technique sont assurées du lundi au vendredi, à l'exclusion des jours fériés, de 9h00 à 12h00 et de 14h00 à 18h00. Les interventions effectuées par le Prestataire en dehors des heures susvisées sont des astreintes non incluses dans le contrat de prestations et qui font l'objet d'une facturation différente de celle prévue au contrat.

Le Prestataire s'engage à prendre en compte les incidents dans un délai raisonnable pendant les horaires de service. Il s'engage à tout mettre en œuvre pour apporter une réponse à la requête du Client sous 24 heures ouvrées.

Dans le cadre d'une intervention technique nécessitant l'intervention préalable d'un autre professionnel, notamment un électricien, le Client devra le faire intervenir sur sa seule initiative et sous sa responsabilité. La responsabilité de la société TRILOG ne pourra être engagée si le délai d'intervention du professionnel entraine un retard dans l'exécution de sa propre prestation.

7.5 Logiciels

Mises à jour

Les nouvelles versions et mises à jour éventuelles des logiciels ne sont pas comprises dans le devis. Elles pourront être commandées auprès de TRILOG, après acceptation préalable d'un nouveau devis.

TRILOG est d'ores et déjà autorisée par le Client à intervenir de sa propre initiative sur les logiciels, sans avertissement préalable, soit en raison de la détection d'une anomalie, soit en cas de modification de l'environnement légal ou règlementaire.

Licence d'utilisation

Les droits d'auteur des logiciels sont protégés par le Code de la propriété intellectuelle. Le client s'engage à respecter strictement les droits de propriété intellectuelle et les licences d'utilisation attachés aux produits vendus.

Le Client s'engage à utiliser chaque logiciel conformément aux dispositions des présentes conditions générales et aux prescriptions d'utilisation contenues dans la documentation remise au Client, et pour les seuls besoins du Client nommément désigné au contrat. Toute utilisation non expressément autorisée par TRILOG ou l'éditeur du logiciel est illicite, conformément à l'article L.122-4 du Code de la propriété intellectuelle.

Il est interdit au Client, et sans que cette liste soit exhaustive, de procéder notamment à :

- Toute reproduction par quelque moyen que ce soit des logiciels et de la documentation,
- Toute représentation, diffusion, ou commercialisation des logiciels, que ce soit à titre onéreux ou gratuit,
- Toute forme d'utilisation des logiciels de quelque façon que ce soit aux fins de conception, réalisation, diffusion ou commercialisation d'un logiciel similaire équivalent ou de substitution,
- Toute adaptation, modification, arrangement des logiciels pour quelque raison que ce soit, notamment en vue de la création d'un logiciel dérivé ou entièrement nouveau ;
- Toute transcription directe ou indirecte, ou traduction dans d'autres langages des logiciels ainsi que leur modification même partielle en vue notamment d'une utilisation sur tout autre produit.

Le droit d'utilisation est accordé pour la version des logiciels disponibles à la date d'entrée en vigueur du contrat, ainsi que pour toutes les mises à jour et nouvelles versions, dans les formes prescrites au paragraphe "Mises à jour" ci-dessus.

Le droit d'utilisation des logiciels est intransmissible et inaliénable et n'a pas pour conséquence de transférer des droits patrimoniaux et moraux y attachés.

Logiciel Kiwi Backup Santé

Le logiciel d'exploitation permet la connexion au serveur de sauvegarde, le transfert crypté des fichiers à sauvegarder et la restauration des Données sur l'ordinateur d'origine ou sur tout autre poste. L'usage du service requiert l'accès préalable au réseau Internet, lequel reste à la seule charge du Client.

TRILOG concède au Client un droit d'utilisation non exclusif sur le logiciel d'exploitation, aux seules fins d'utilisation de la Solution de sauvegarde de Données Kiwi Backup Santé.

La licence d'exploitation est consentie pour toute la durée de l'abonnement souscrit par le Client.

Toute modification du logiciel, transcription et, d'une manière générale, toute opération nécessitant l'usage des sources et de leur documentation sont exclusivement réservées à Kiwi Backup.

Lors de chaque connexion à l'interface d'administration (en option), le Client utilisera les identifiants qui lui auront été communiqués.

Le Client s'engage à mettre en œuvre une politique de sécurité des mots de passe et notamment conserver le secret de ses identifiants et à ne pas les divulguer sous quelque forme que ce soit.

Le Client est entièrement responsable de l'utilisation des identifiants et il est responsable de la garde des mots de passe qui lui sont remis. Il s'assurera qu'aucune autre personne non autorisée par TRILOG n'a accès au logiciel et à ses fonctionnalités.

En cas de perte ou de vol ou de retrait des identifiants, le Client en informera TRILOG par courriel. TRILOG invalidera alors l'accès et communiquera un nouveau mot de passe au Client.

TRILOG ne saurait être tenu responsable de la destruction accidentelle des Données par le Client ou un tiers ayant accédé aux fonctionnalités du logiciel au moyen des identifiants remis au Client.

Kiwi Backup pourra effectuer des mises à jour du logiciel de sauvegarde afin d'améliorer le service ou de proposer de nouvelles fonctionnalités. Les mises à jour logicielles sont appliquées automatiquement, sans que le Client ait besoin d'intervenir.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

En cas de telles modifications, le Client sera informé par courriel par TRILOG.

Le cas échéant, TRILOG s'engage à informer (par courriel) le Client en cas de suppression d'un service en tenant compte d'un préavis de 3 mois.

Kiwi Backup se réserve la possibilité pour des raisons de nécessité de maintenance des serveurs d'interrompre tout ou partie du service sans information préalable.

Kiwi Backup se réserve le droit de faire évoluer son infrastructure informatique sans altérer le service tel que défini dans le présent Contrat afin d'assurer la qualité, la performance et la sécurité de la prestation**.** Kiwi Backup se réserve expressément toute modification, correction ou adaptation du logiciel d'exploitation y compris en vue d'assurer son interopérabilité.

Kiwi Backup mettra tout en œuvre pour que ces évolutions aient le minimum d'impact en termes de disponibilité du service et d'intégrité des Données sauvegardées.

Toute modification du lieu d'Hébergement sera notifiée au Client par l'intermédiaire de TRILOG. Pour garantir le bon fonctionnement des Services souscrits et le bon respect des processus convenus, le Client reconnaît toute liberté à Kiwi Backup pour déplacer ses Données sur le territoire de l'Union Européenne.

Considérant les obligations du Client en sa qualité de responsable des traitements de Données à caractère personnel contenu dans son Environnement auprès de ses propres clients et utilisateurs et auprès de la Commission Nationale Informatique et Libertés (Cnil), TRILOG devra obtenir l'autorisation expresse de déplacer les Données du Client hors du territoire de l'Union Européenne. Ceci afin que Kiwi Backup puisse intervenir.

Kiwi Backup s'engage à ce que les Services et l'accès à l'Infrastructure Client ne subisse aucune perturbation du fait d'un quelconque déménagement.

Dans le cadre de l'évolution du service et sous réserve de maintien du niveau de service au moment de la signature du contrat, Kiwi Backup a la possibilité de changer le sous-traitant hébergeur sans obligation d'informer TRILOG et le Client ou sans sollicitation de leurs accords préalables. Le Règlement Européen sur la Protection des Données (RGPD) imposant la transparence de la sous-traitance, TRILOG s'engage à informer le Client du choix du sous-traitant hébergeur nouvellement sélectionné par Kiwi Backup.

ARTICLE 8 – PRESTATION DE SAUVEGARDE EXTERNALISEE DE DONNEES

TRILOG propose les modules suivants, qui permettent un accès à un serveur de données via Internet et un service de stockage et de restauration de données, sauvegardées par le Client :

- un module Kiwi backup Santé par l'intermédiaire de son prestataire la société Kiwi Backup (44917956300050 - 40, rue Victor Schoelcher 68200 Mulhouse),

- un module ACRONIS BACKUP CLOUD par l'intermédiaire de son prestataire la société HERMITAGE SOLUTIONS (3 Rue de l'Arbre Sec – 69001 LYON). Le Client qui souhaite bénéficier de cette prestation doit créer un compte à son nom sur la plate-forme ACRONIS à l'adresse communiquée par TRILOG. Le Client est tenu d'accepter et de respecter les conditions générales d'utilisation de ladite plate-forme et engage sa responsabilité en cas de non-respect de ces dernières, sans que la responsabilité de TRILOG ne puisse être recherchée.

TRILOG, Kiwi Backup et HERMITAGE SOLUTIONS n'exercent aucun contrôle ni surveillance sur les fichiers qui leur sont confiés, lesquels demeurent la propriété du Client et restent confidentiels.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

8.1 FONCTIONNEMENT DE LA SOLUTION DE SAUVEGARDE

La solution de sauvegarde proposée par TRILOG par l'intermédiaire de ses prestataires susvisés est conforme à la législation française en vigueur. TRILOG décline toute responsabilité dans l'hypothèse où la solution de sauvegarde de données ne respecterait pas la législation du pays d'utilisation autre que la France.

La sauvegarde de données est effectuée uniquement pour le compte du Client qui souscrit une option de sauvegarde externalisée des données.

Le Client est seul responsable du choix des Données à sauvegarder, des horaires de sauvegarde ainsi que du respect des règles de sauvegarde particulières de certains fichiers, notamment les bases de Données nécessitant l'arrêt du logiciel pour être sauvegardées, boîtes aux lettres mail.

Le Client doit vérifier le bon déroulement des sauvegardes, par l'intermédiaire de l'interface d'administration, s'il en a l'accès, ou des courriels de rapport automatiques. Le Client s'engage à respecter les conditions d'usage des droits d'utilisation qui leur sont concédées par les présentes.

Il est recommandé de procéder régulièrement à des tests de restauration et de bonne réutilisation des Données sauvegardées.

Kiwi Backup met en place un observatoire quotidien des sauvegardes. Si une connexion ou un transfert programmé n'a pas eu lieu, une alerte est envoyée à l'adresse email fournie par le Client. Le Client est seul responsable de la suite qu'il souhaite donner à ces messages d'alerte.

Le client est tenu d'informer la société TRILOG de toute modification de l'emplacement des données à sauvegarder. A défaut, la responsabilité de la société TRILOG ne pourra être engagée en cas de défaillance de la sauvegarde.

Le Client est tenu de collaborer de bonne foi, et de s'assurer de la collaboration de son personnel et de tous prestataires tiers dont l'intervention est requise pour la réalisation de la prestation objet du Contrat avec TRILOG afin de permettre à cette dernière d'exécuter les prestations conformément aux documents contractuels.

Le Client s'engage à mettre à disposition de TRILOG, après avoir vérifié leur exactitude, toute donnée nécessaire ou utile à l'exécution des prestations au cours de la vie du Contrat. Il s'engage également à répondre en temps utile aux questions posées par TRILOG.

Le Client a la responsabilité de l'expression de son besoin et sera tenu d'informer TRILOG des évolutions nécessaires à l'exercice de son activité.

Le Client s'engage à ce que les données sauvegardées soient conformes aux normes en vigueur, licites et qu'elles respectent le droit des tiers. La Société n'est pas responsable de la nature et du contenu des données sauvegardées qui relèvent de la seule responsabilité du Client.

La sauvegarde individualisée permet une restitution ou une restauration sélective d'une ou plusieurs données sauvegardées sans avoir besoin de procéder à une restauration complète du serveur. Le Client est informé qu'en cas d'incident, seules les données figurant sur cette liste pourront être restaurées ou restituées.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

8.2 PREREQUIS TECHNIQUES - MAINTENANCE

Le service ne peut être activé sans les prérequis suivants :
- un serveur
- une ligne Internet fiable et un débit suffisant.

Les choix techniques d'intervention, les manipulations à distance, les Données transmises, etc. sont de la responsabilité exclusive du Client qui déclare avoir été informé suffisamment des procédures techniques et de sécurité que comporte le système notamment en matière de fiabilité des Données transmises. Le Client s'engage à s'assurer que son équipement informatique est compatible avec les logiciels fournis dans le cadre de la prestation.

L'opérateur de télécommunications gérant le réseau est choisi par le Client conformément aux spécifications requises pour le bon fonctionnement du Service.

Le Client est averti des aléas techniques inhérents à l'Internet et des interruptions d'accès pouvant en résulter.

En conséquence, TRILOG ne peut pas être tenu pour responsable des interruptions du réseau entraînant d'éventuelles indisponibilités ou ralentissements de l'accès et du fonctionnement du Service souscrit en lien avec le réseau choisi par le Client.

Dès lors, TRILOG a attiré l'attention du Client sur l'importance du choix de l'opérateur de télécommunications et notamment des options de secours qu'il peut offrir par la mise en place d'une ligne parallèle en cas d'interruption du réseau.

De même, TRILOG ne pourra en aucun cas être tenu pour responsable de tout dommage en cas de préjudice causé par une interruption ou une baisse de Service de l'opérateur de télécommunications, du fournisseur d'électricité ou en cas de force majeure

La maintenance du système pourra nécessiter des interventions à distance ou sur place. Le Client s'engage à laisser libre accès aux préposés de TRILOG à l'ensemble de son installation informatique. Toute intervention consécutive à une panne qui ne relèverait pas des prestations que la société TRILOG s'est engagée à fournir sera facturée au Client en supplément.

Le Client doit veiller à la protection et au bon fonctionnement de ses matériels informatiques et des connexions permettant la sauvegarde. La Société décline toute responsabilité si la sauvegarde est empêchée par la détérioration ou le dysfonctionnement des matériels du Client ou tout élément extérieur indépendant de sa volonté (sinistre, panne électrique, connexion impossible etc.….) et ce, pendant toute la durée du dysfonctionnement ou de l'incident.

Le Client doit donc veiller à ce que les matériels et pré requis ci-dessus listés soient en parfait état de fonctionnement au moment de la sauvegarde fixé par les parties.

Le Client s'engage à garantir TRILOG des conséquences (dommages, frais de procédure etc.…) de tout recours d'un tiers, de tout litige ou de toute procédure, civile ou pénale engagée contre la Société et tirée de la nature ou du contenu des données sauvegardées. Conformément aux dispositions en vigueur, TRILOG pourra mettre les données sauvegardées à la disposition de toute autorité judiciaire compétente et autorisée et pourra, sur réquisition ou décision de justice, supprimer l'accès aux données ou procéder à leur destruction. Tous les frais engagés dans ce cadre par TRILOG seront alors refacturés au Client.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

La restitution des données interviendra sous 24 heures ouvrées sur simple demande écrite du Client adressée à TRILOG. Si la restitution implique une restauration des données directement sur le serveur par une intervention sur place, et si le client n'a pas parallèlement souscrit un contrat maintenance sur le serveur concerné par le sinistre auprès de TRILOG, la restauration sur place interviendra sur devis accepté par le Client. Le Client reconnaît et accepte que les données restituées ou restaurées seront celles enregistrées lors de la dernière sauvegarde réalisée avant sa demande de restauration. Les données enregistrées par le Client sur son serveur entre la dernière sauvegarde et l'incident ne pourront être restituées ou restaurées, ce que le Client reconnaît et accepte.

8.2. SECURITE DES DONNEES

TRILOG s'engage à mettre en œuvre les moyens techniques appropriés pour assurer la sécurité des Données.

TRILOG s'engage à préserver l'intégrité et la confidentialité des Données contenues dans les fonctionnalités du logiciel.

TRILOG mettra en place les mesures techniques et organisationnelles de nature à empêcher tout accès ou utilisations fraudeuses des Données.

TRILOG n'exerce aucun contrôle ni surveillance sur les fichiers qui lui sont confiés, lesquels demeurent la propriété du Client et restent confidentiels.

Les données temporaires créées lors des sauvegardes sont conservées pour la durée du traitement et supprimées au plus tard 1 mois après leur création.

8.3. CONFORMITE DES SERVICES

TRILOG s'engage pour ses Services de sauvegarde externalisée de données à mettre en œuvre tous les moyens dont il dispose pour assurer au mieux la sauvegarde des Données contenues sur les ordinateurs connectés.

Kiwi Backup et HERMITAGE SOLUTIONS garantissent, conformément aux dispositions légales, le Client, contre tout défaut de conformité des Services et tout vice caché, provenant d'un défaut de conception ou de fourniture desdits Services à l'exclusion de toute négligence ou faute du Client. La responsabilité de Kiwi Backup, d'HERMITAGE SOLUTIONS et de TRILOG ne pourra en aucun cas être engagée en cas de retard ou de suspension de la fourniture de la prestation imputable au Client, ou en cas de force majeure telle que définie par l'article 1218 du Code civil.

La responsabilité de TRILOG ne peut être engagée qu'en cas de faute ou de négligence prouvée, et est limitée aux préjudices directs à l'exclusion de tout préjudice indirect, de quelque nature que ce soit. Les besoins non exprimés par le Client sont exclus du champ de la responsabilité de TRILOG.

Afin de faire valoir ses droits, le Client devra, sous peine de déchéance de toute action s'y rapportant, informer TRILOG, par écrit, de l'existence des vices dans un délai maximum de 15 jours à compter de leur découverte. Kiwi Backup ou HERMITAGE SOLUTIONS rectifiera ou fera rectifier, à ses frais exclusifs, selon les modalités adéquates et agréées par le Client, les Services jugés défectueux. En tout état de cause, au cas où la responsabilité de Kiwi Backup ou HERMITAGE SOLUTIONS serait retenue, la garantie de TRILOG serait limitée au montant HT payé par le Client pour la fourniture des Services.

TRILOG s'engage à fournir au Client des interfaces ainsi qu'un support technique en langue française.

8.4. MOYENS MIS EN ŒUVRE ET OBLIGATION D'INFORMATION ET DE CONSEIL

TRILOG s'engage à mettre en place les moyens humains et matériels nécessaires à la bonne exécution des tâches et missions.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Le cas échéant, TRILOG s'engage à collaborer avec les autres prestataires du Client dans la mesure nécessaire à l'exécution des prestations et sous la direction du Client.

TRILOG s'engage à fournir au Client une assistance de premier niveau sur demande de ce dernier dans les modalités définies par l'article 12.

TRILOG est débiteur d'une obligation d'information et de conseil envers le Client.

Il informera le Client de tout évènement porté à sa connaissance, qui pourrait perturber l'exécution de la prestation, ainsi que de toute évolution éventuellement nécessaire.

8.5 REVERSIBILITE

8.5.1 Principe

En cas de cessation de relation contractuelle, quelle qu'en soit la cause, TRILOG s'engage, à la demande du Client exprimée dans les formes et délais précisés au point précédent, à :

- une réversibilité du processus d'exploitation du système d'information ;
- détruire à la demande du Client l'ensemble des Données hébergées lui appartenant;
- maintenir le service de restauration actif pendant 90 jours pour la solution Kiwi Backup Santé de sorte que le Client puisse avoir accès à ses sauvegardes le temps de mettre en place une autre solution. A l'issue de cette période, TRILOG supprimera les Données de sauvegarde du Client.

En outre, le Client ayant toute latitude pour réaliser les restaurations de données nécessaires pendant la période décrite ci-avant, il est spécifié qu'aucune donnée ne pourra être fournie au Client par TRILOG sur quelque support amovible que ce soit.

TRILOG s'engage à fournir au Client qui en fait la demande, au moins 3 mois précédant la date d'expiration effective du Contrat, les informations qui lui seraient nécessaires pour lui permettre de préparer la mise en œuvre de la réversibilité.

Si le Client souhaite engager une procédure de réversibilité, il doit en informer TRILOG, par lettre recommandée avec accusé de réception, dans un délai maximum de (un) 1 mois à compter de la réception de la lettre de résiliation du Contrat.

A défaut, les Données du Client ne pourront plus être récupérées, et cela sans que la responsabilité de TRILOG ne puisse être engagée.

8.5.2 Mise en œuvre

TRILOG s'engage à mettre en œuvre les moyens raisonnables appropriés à une totale réversibilité, que ce soit au profit du Client ou de tout autre prestataire qui se substituerait au Client.

Le Client collaborera activement avec TRILOG dans ce but.

Les prestations liées à la réversibilité étant fournies après la cessation de la relation contractuelle, les parties s'accordent sur le fait que la présente clause survivra à la disparition du Contrat pour quelque cause que ce soit.

Un plan de réversibilité détaillé, sera élaboré, dans un délai maximum de trois 3 mois à partir de la notification de souhait d'engager la procédure de réversibilité, conjointement par les parties en Comité de Pilotage. Ce plan de réversibilité comportera :

- La description précise des tâches à accomplir par les deux parties ;
- Un échéancier desdites tâches ainsi que leurs conditions financières.

Les parties reconnaissent que les conditions financières ne peuvent être définies qu'au moment de la sortie du Contrat, au vu des prestations à effectuer et de la difficulté du transfert selon les solutions et/ou format demandés par le Client.

TRILOG fera en sorte que le Client puisse poursuivre l'exploitation des Données sans rupture, directement ou avec l'assistance d'un autre prestataire. Les prestations de réversibilité sont réalisées de sorte à assurer le transfert des Données Client hébergées par TRILOG vers une nouvelle plateforme désignée par le Client. Ce transfert de Données permet la reprise par le Client ou tout tiers désigné par lui de l'application et des Données fournis par le Client.

Pour ce faire, TRILOG, sauf accord écrit et préalable du Client, s'engage à ne mettre en œuvre que des solutions largement diffusées tant en France qu'à l'étranger ; non spécifiques et conformes aux règles de l'art ; facilement portables, c'est-à-dire pouvant être transférées, à fonctionnalités identiques, sur un autre système conforme à l'état de l'art sans nécessiter de modifier sensiblement l'organisation et le format de Données du Client.

TRILOG s'engage à l'expiration du Contrat :

- à restituer au Client les moyens matériels et logiciels, ainsi que les Données confiés par le Client et, plus généralement ;
- à restituer au Client tout élément qui aurait été mis à la disposition de TRILOG par le Client dans le cadre de la fourniture des prestations ;
- à ne conserver aucune copie des éléments composant l'Environnement du Client et à les effacer définitivement de ses serveurs.

Pour sa part le Client s'engage à restituer à TRILOG tout élément (matériels, logiciels) que ce dernier lui aura mis à disposition dans le cadre de la fourniture des prestations, sauf reprise ou rachat par le Client.

ARTICLE 9 – MAINTENANCE

TRILOG s'engage, dans les conditions ci-après définies, à effectuer un diagnostic de tout matériel défectueux faisant l'objet d'un contrat de maintenance. Il sera procédé à la réparation ou, le cas échéant au remplacement du seul matériel sous garanti.

TRILOG intervient en 24 heures ouvrées à compter de la réception de l'appel du Client pendant les horaires de permanence téléphonique mentionnés à l'article 7.4 pour signaler la panne à réparer. TRILOG ne pourra être tenue pour responsable des dommages consécutifs à un retard dans l'intervention qu'en cas de perte majeure de service pour le Client et en tout état de cause pour un retard supérieur à 48 heures. Lors de son intervention, TRILOG conseillera au client le meilleur choix à opérer entre la réparation et le remplacement des matériels défectueux. Sa responsabilité sera définitivement dégagée si le Client ne suit pas son avis. Les délais de remplacement et/ou de réparation des matériels défectueux par TRILOG dépendront des stocks disponibles et/ou des délais de livraisons de ses fournisseurs et /ou de la complexité de la panne. Lors de son intervention, la société indiquera au Client un délai pour la réparation ou le remplacement du matériel. Ce délai ne pourra qu'être indicatif et le client ne pourrait en aucun cas tirer grief d'un éventuel retard.

En cas de panne du matériel garantie non résolue dans les 48h ouvrables, il sera prêté un matériel permettant au client de continuer son activité. Il ne sera cependant pas procédé à la réinstallation des logiciels spécifiques non indispensables à l'activité du client.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Le Client aura la garde des produits et matériels qui lui seront prêtés avec toutes les conséquences de droit qui en découlent. Il devra notamment les assurer contre tout risque de perte, vol, ou dégradation, et les utiliser conformément aux instructions d'utilisations. A défaut pour le Client de restituer ces matériels dans l'état qui lui avaient été confiés, TRILOG serait fondée à lui réclamer le prix nécessaire pour leur remplacement ou leur réparation.

Sont exclus de la prestation de maintenance :

• Les matériels non désignés au contrat ; • Les dommages résultant notamment d'un accident, d'une négligence, d'une malveillance, d'une utilisation impropre aux prescriptions techniques du constructeur, d'un défaut du réseau électrique, d'une intervention pratiquée sur le matériel du fait du Client ou d'un tiers et plus généralement de tout dommage dont l'origine est étrangère au matériel lui-même ;
• la réalisation sur le matériel de modifications techniques par le Client lui-même ou des tiers ;
• la réparation ou le remplacement de tout élément du matériel connecté à d'autres matériels, non conformes aux spécifications techniques du constructeur ;
• la réparation ou le remplacement des installations électriques extérieures au matériel ou de tout autre élément périphérique
• le remplacement des consommables (cartouches, têtes d'impression…) ; et des kits de maintenance constructeur ;
• les pannes résultant d'un virus ;
• la mise à jour et l'assistance des logiciels ;
• le changement des batteries de portables et des batteries d'onduleurs.

Dans les cas ci-dessus, toute intervention de la Société fera l'objet d'un devis et d'une facturation distincte.

Le Client n'ayant pas souscrit un contrat de sauvegarde externalisée de données devra effectuer et conserver, sous sa seule responsabilité, au moins une copie de sauvegarde de ses données et programmes, avant toute intervention de la société TRILOG.

La société n'est aucunement responsable de la réalisation effective par le Client de la sauvegarde de ses données ou des incidents matériels et/ou informatiques susceptibles de survenir à l'occasion des opérations de sauvegarde réalisées par le Client. Sauf faute caractérisée, TRILOG ne pourra être tenue pour responsable en cas de perte ou de destruction des programmes et des données qui pourraient survenir lors d'un incident de quelque nature que ce soit à l'occasion de la réalisation de sa mission de maintenance.

ARTICLE 10 – OBLIGATIONS DU CLIENT

Le Client s'engage à donner accès au Prestataire à toutes les informations jugées nécessaires par ce dernier pour assurer les prestations commandées. Tout retard dans la communication desdits éléments reporterait d'autant la date de livraison ou d'exécution des prestations, sans que ce retard ne puisse être imputé au Prestataire.

Le Client a connaissance que les modalités de fourniture des prestations pourront faire l'objet d'ajustements en cours d'exécution afin de permettre au Prestataire de mener à bien sa mission.

Le Client a connaissance que les modules informatiques mis en place par le Prestataire pourront faire l'objet de mises à jour indispensables à leur utilisation.

Le Client assume l'entière responsabilité concernant : l'adéquation des progiciels à ses besoins, la qualification et la compétence de son personnel, l'ensemble des obligations lui incombant au titre de la sauvegarde et de l'archivage de ses données.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

En cas de perte ou vol des matériels mis à disposition par TRILOG, le Client devra immédiatement informer TRILOG afin de suspendre l'usage impropre du service. Le client notifiera l'événement de perte ou de vol à TRILOG par lettre recommandée avec accusé de réception en y joignant la plainte déposée auprès des autorités compétentes. Le Client devra remplacer aussitôt le matériel perdus ou volé, et à ses frais : l'immobilisation ou la disparition de ceux-ci ne donnant droit à aucune suspension ou réduction dans le paiement des prestations.

La location ou la mise à disposition des matériels ne confère aucun droit de propriété sur ceux-ci et le Client doit veiller à leur entretien et à leur conservation au sens de l'article 1242 du Code civil. A cette fin, le Client s'oblige à souscrire une police d'assurance le garantissant des risques de détérioration, destruction ou disparition, notamment en cas de bris perte ou vol, vandalisme, incendie ou explosion. Le paiement des loyers ou des redevances ne pourra en aucun cas être différé ou interrompu à ce titre. Le client d'interdit de louer, prêter, transférer ou distribuer tout ou partie, extrait, sélection, arrangement, adaptation, compilation ou dérivés des produits loués ou sous licence à un tiers.

Les accessoires et consommables (batterie, bloc d'alimentation, bobines, adaptateur USB, prises et câbles etc…) ne sont couverts ni par la garantie ni par la « Maintenance ».

ARTICLE 11 – GARANTIE ET LIMITATION DE RESPONSABILITE

11.1 Conditions générales

Le Prestataire garantit le Client contre tout défaut de conformité des matériels et tout vice caché, provenant d'un défaut de conception ou de fabrication des matériels et les rendant impropres à leur usage, à l'exclusion de toute négligence ou faute du Client, pendant la durée indiquée sur le devis, le bon de commande et le bon de livraison.

Afin de faire valoir ses droits, le Client devra, sous peine de déchéance de toute action s'y rapportant, informer le Prestataire, par écrit, de l'existence des vices dans un délai maximum de dix (10) jours à compter de leur découverte.

Il est expressément convenu qu'après l'expiration de ce délai de 10 jours l'acheteur ne pourra invoquer la non-conformité des produits, ni opposer celle-ci en demande reconventionnelle pour se défendre à l'occasion d'une action en recouvrement de créance engagée par notre société.

A défaut du respect de ces conditions, la responsabilité de notre société vis-à-vis de l'acheteur, à raison d'un vice caché, ne pourra être mise en cause.

11.2 Matériels

Le Prestataire remplacera ou fera réparer les matériels ou pièces sous garantie jugés défectueux. Cette garantie couvre également les frais de main d'œuvre.

La garantie sur site, si elle est contractée, comprend l'unité centrale et l'écran, pièces, main d'œuvre et déplacements compris, sauf exclusion particulière prévue sur le devis ou l'offre acceptée. En cas de panne du matériel garanti non résolue sous 48 heures ouvrées, le Prestataire s'engage à prêter au Client un matériel permettant à ce dernier de poursuivre son activité. Il ne sera cependant pas procédé à la réinstallation des logiciels spécifiques non indispensables à l'activité du client.

La garantie ne s'applique pas aux consommables et ne s'appliquera pas en cas d'utilisation anormale ou non conforme aux usages du matériel.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Le remplacement des matériels ou pièces défectueux n'aura pas pour effet de prolonger la durée de la garantie ci-dessus fixée.

Les défauts ou détériorations des matériels livrés consécutifs à des conditions anormales de stockage et/ou de conservation et/ou d'utilisation chez le Client ne pourront ouvrir droit à la garantie due par le Prestataire.

Est exclu de cette garantie tout dysfonctionnement qui trouverait son origine dans la fourniture d'une prestation ou d'une intervention effectuée par une tierce partie.

11.3 Prestations

Le Prestataire garantit que sa prestation est fournie avec toute la diligence et la compétence raisonnablement requise, et exclut toute autre garantie non stipulée explicitement. Il est soumis à une obligation de moyens.

Le Prestataire rectifiera ou fera rectifier, à ses frais exclusifs, les services jugés défectueux.

La garantie du Prestataire est limitée au montant HT payé par le Client pour la fourniture des prestations. Est exclu de cette garantie tout dysfonctionnement qui trouverait son origine dans la fourniture d'une prestation ou d'une intervention effectuée par une tierce partie ou dans l'utilisation de consommables compatibles.

Le Prestataire ne saurait voir sa responsabilité engagée en cas de dommages de quelque nature que ce soit subis par le Client ou des tiers et résultant directement ou indirectement d'une de ses prestations ou l'utilisation d'un de ses logiciels, notamment la perte de données ou toute perte financière résultant de son utilisation ou de l'impossibilité de l'utiliser.

Le Prestataire ne peut être tenu pour responsable d'infraction aux lois françaises et internationales de protection de la propriété intellectuelle, pour tous travaux, modifications, réalisations effectués à partir de tout élément de toutes sortes fournis par le Client tels que textes, photographies, logos, images, graphisme dont il n'aurait pas la propriété exclusive.

Dans le cas où la responsabilité du Prestataire se trouverait engagée par suite d'un défaut de respect de ses obligations, que ce soit sur une base contractuelle, extracontractuelle, ou pour toute autre raison, sa responsabilité est limitée aux dommages directs subis par le Client. Les frais d'expertise éventuels seront supportés par moitié entre le Client et le Prestataire.

Le Prestataire ne sera en aucun cas tenu d'indemniser d'éventuels dommages, de quelque nature que ce soit, résultant :

- d'une utilisation non-conforme au but de tout logiciel, service, ou prestation
- de l'utilisation de consommables compatibles
- de tout cas de force majeure, notamment la foudre, le dysfonctionnement des moyens de télécommunication ou la rupture de la fourniture d'énergie
- de tout fait qui peut être démontré comme se situant hors du champ des responsabilités du Prestataire

11.4 Sauvegarde de données

Pour les clients ayant contracté un service de sauvegarde de données, la société TRILOG s'engage à mettre en œuvre tous les moyens dont elle dispose pour assurer au mieux la sauvegarde des données.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

L'engagement de TRILOG consiste exclusivement en la mise à disposition du service, à l'exclusion de toute garantie de résultat quant au choix des données sauvegardées par le Client.

Dans tous les cas, TRILOG n'aura aucune obligation à l'égard du Client, notamment en cas de dysfonctionnent ou de difficultés de toute nature susceptibles de survenir au niveau des équipements, réseaux, manipulation ou logiciels du client.

Les choix techniques d'intervention, les manipulations à distance, les données transmises, etc. sont de la responsabilité exclusive du Client qui déclare avoir été informé suffisamment des procédures techniques et de sécurité que comporte le système notamment en matière de fiabilité des données transmises.

De même, TRILOG n'assume aucune responsabilité quant à la qualité technique des réseaux de communication utilisés pour les liaisons. La maintenance des moyens informatiques et de télécommunication permettant l'accès au service restent entièrement à la charge du client qui reconnaît avoir été suffisamment informé de la configuration nécessaire et des modalités liées à l'utilisation du service.

A ce titre, TRILOG ne peut garantir la continuité du service pour des cas de coupures du réseau internet du CLIENT.

Si une connexion ou un transfert programmé n'a pas eu lieu, une alerte est envoyée à l'adresse email fournie par le Client. Le Client est seul responsable de la suite qu'il souhaite donner à ces messages d'alerte, ainsi que du bon fonctionnement et de la mise à jour de l'adresse email fournie. La responsabilité de la société TRILOG ne pourra être engagée en cas de défaillance du système de sauvegarde si le Client ne l'a pas informé de la réception du message d'alerte susvisé ou de son changement d'adresse email ou de tout dysfonctionnement sur l'adresse fournie.

La responsabilité de TRILOG ne pourra pas être engagée en cas :

- de non-respect par le Client des procédures d'utilisation définies par TRILOG
- d'inexécution ou de mauvaise exécution du Contrat due, soit au fait du Client, soit au fait insurmontable et imprévisible d'un tiers au Contrat, soit à la force majeure. Dans de telles circonstances, TRILOG sera dispensé de l'exécution de ses obligations dans la limite de cet empêchement, de cette limitation ou de ce dérangement,
- de non-conformité du produit à la législation du pays du Client, auquel il appartient de vérifier si le produit n'est pas interdit à la vente dans son pays,
- de faute, négligence ou omission d'un tiers sur lequel TRILOG n'a aucun pouvoir de contrôle de surveillance.
- - en cas de force majeure ou de faits indépendants de la volonté de TRILOG (notamment en cas de défaillance électrique, d'interruption du réseau, de défaillance du matériel de réception ou de la ligne du Client, de manque de fiabilité de la transmission des données sur réseau ou de tout autre préjudice subi de ce fait par le client).

La force majeure entraîne, pendant la durée de sa survenance, la suspension des obligations nées du présent contrat. Toutefois, si le cas de force majeure avait une durée supérieure à TROIS (3) mois, il ouvrirait droit à la résiliation du contrat de prestations de sauvegarde de données par l'une ou l'autre des Parties par Lettre Recommandée avec AR.

Le Client ne pourra, en aucun cas, engager la responsabilité de TRILOG dans l'hypothèse, notamment par le biais d'un appel en garantie, où un patient ou un ayant droit devait agir contre le Client, et/ou ses préposés et/ou partenaires, du fait d'actes de prévention, de diagnostic, de soins, et plus généralement de tout acte portant atteinte à l'intégrité physique ou morale des personnes.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Le Client est parfaitement conscient qu'il est pleinement responsable des conséquences de son activité et que le Service mis à disposition par TRILOG ne pourra être considéré autrement que comme un simple outil s'appuyant sur les informations que le Client implémente lui-même dans le Service précité.

TRILOG ne prend pas en charge l'indemnisation des dommages indirects et immatériels tels que notamment le préjudice moral ou la perte de bénéfice. Il appartient au Client de souscrire à ses frais les polices d'assurances appropriées.

Les parties conviennent expressément que tout préjudice financier ou commercial (tel que pertes de bénéfices, pertes de commandes, troubles commerciaux quelconques), ou toute action dirigée contre le Client par un tiers constitue un dommage indirect et n'ouvre pas droit à réparation par TRILOG, même si cette dernière a été avisée de la possibilité de survenances de tels préjudices.

TRILOG ne pourra en aucun cas être tenu pour responsable des préjudices indirects subi par le Client qui pourraient survenir du fait ou à l'occasion de l'exécution du présent Contrat et de ses suites.

Dans le cas où la responsabilité de TRILOG serait retenue, il est expressément convenu que le total des indemnisations qui serait mises à sa charge, toutes causes confondues, ne pourrait pas dépasser le montant annuel du prix de l'abonnement.

ARTICLE 12 - RESILIATION

En cas de manquement par le Client à l'une de ses obligations essentielles, notamment en cas de non-paiement du prix, le Prestataire sera autorisé trente (30) jours après une mise en demeure adressée par Lettre Recommandée avec AR restée sans effet, à résilier de plein droit le contrat par simple envoi d'une Lettre Recommandée avec AR, nonobstant le droit de demander réparation du préjudice subi. Le contrat prendra alors fin à la date d'envoi de cette dernière Lettre Recommandée.

Le Client devra s'acquitter de l'ensemble des sommes restant dues jusqu'à la fin de la période contractuelle. Tout acompte éventuel restera acquis au Prestataire à titre de première indemnité, sans préjudice de tout autre dommage et intérêt.

ARTICLE 13 – FORCE MAJEURE

Est considéré comme évènement de force majeure tout évènement imprévisible, irrésistible et extérieur à la société TRILOG. Ainsi à titre d'exemple sont considéré comme évènement de force majeure ou cas fortuit, les grèves partielles ou totales, internes ou externes à l'entreprises, le lock-out, les intempéries, épidémies, blocage des moyens de transport ou d'approvisionnement, tremblement de terre, incendie, tempête, inondation, dégâts des eaux, restriction gouvernementale ou légale, modification légale ou règlementaire des formes de commercialisation.

ARTICLE 15 - CONFIDENTIALITE

Toutes les informations échangées entre le Client et le Prestataire ou dont ils auraient connaissance à l'occasion de la préparation et de l'exécution du contrat, quel que soit leur support, présentent un caractère strictement confidentiel. Chacune des parties s'engage à les protéger et à ne pas les divulguer à des tiers sans l'autorisation préalable et écrite de l'autre partie. Les parties s'engagent à respecter les obligations résultant du présent article pendant toute la durée du contrat et pendant les 5 ans suivant sa cessation.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

ARTICLE 16 – TRAITEMENT DES DONNEES PERSONNELLES

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la règlementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement Européen sur la protection des données (UE 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018).

Le Client s'engage, en sa qualité de responsable du traitement, à collecter et à traiter toute donnée à caractère personnel en conformité avec la réglementation en vigueur applicable au traitement de ces Données et notamment au Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978, ainsi qu'au Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016.

Le Client reconnaît avoir été informé par TRILOG de la nécessité d'effectuer des formalités préalables auprès de la Commission Nationale Informatique et Libertés en sa qualité de responsable du traitement, afin de rendre licite le traitement de Données à caractère personnel hébergé par TRILOG.

TRILOG ne saurait être tenu pour responsable du non-accomplissement de ces formalités par le Client, étant entendu que toute l'information utile a été apportée au Client.

Par ailleurs, le Client s'interdit strictement l'utilisation des Services mis à sa disposition pour stocker des fichiers, Données ou applications de toute forme, dont le contenu serait en infraction avec la Loi et les Règlements en vigueur. TRILOG dispose à ce titre de tous recours contre le Client.

Le Prestataire a la qualité de sous-traitant au sens dudit règlement européen. Il est autorisé à sauvegarder pour le compte du Client les données à caractère personnel pour fournir les prestations de services de maintenance informatique, de dépannage, d'assistance et de sauvegarde pendant toute la durée du contrat. L'effacement des données ne pourra être sollicité pendant la durée d'exécution des prestations confiées à TRILOG. La nature des opérations réalisées sur les données, la ou les finalités du traitement, les données à caractère personnel traitées et les catégories de personnes concernées sont mentionnées en annexe du devis ou aux conditions particulières du contrat.

Toutes les prestations fournies par TRILOG sont soumises aux dispositions dudit règlement, dont les clauses particulières applicables sont annexées aux présentes conditions générales.

La déclaration de confidentialité d'ACRONIS pour les utilisateurs du module ACRONIS BACKUP CLOUD est consultable à l'adresse suivante : https://www.acronis.com/fr-fr/company/privacy.html.

ARTICLE 17 – DISPOSITIONS DIVERSES

17.1 Sous-traitance

Le Client autorise expressément le Prestataire à avoir recours, sans formalité préalable, à des partenaires pour tout ou partie de l'exécution des commandes.

17.2 Non-débauchage

Le Client s'engage pendant toute la durée du contrat et 12 mois après la fin de celui-ci, à ne pas démarcher, recruter, ni faire travailler directement ou indirectement un membre du personnel du Prestataire, sauf autorisation écrite et préalable de ce dernier.

17.3 Références commerciales

Le Client autorise expressément le Prestataire à faire figurer son nom et son logo dans ses références commerciales communiquées au public sur tout support, sauf refus expressément notifié du Client.

17.4 Incessibilité

Le contrat de vente ou de prestations ne pourra en aucun cas être cédé, totalement ou partiellement, à titre gratuit ou onéreux, à un tiers par le Client, sauf accord préalable et écrit du Prestataire. Le Prestataire se réserve la possibilité de céder le bénéfice du contrat à toute personne morale qui reprendra l'intégralité des obligations contractées au profit du Client.

ARTICLE 18 – DROIT APPLICABLE – ATTRIBUTION DE JURIDICTION

Les présentes Conditions Générales de Vente sont régies par la loi française et soumises à la juridiction exclusive des tribunaux français. Tout différend relatif aux présentes Conditions Générales de Vente sera soumis à la médiation avant toute saisine du juge. Le médiateur sera désigné par le centre de médiation commerciale de GRENOBLE sis 1, Place André Malraux à GRENOBLE saisi à la requête de la partie la plus diligente. Le médiateur dispose d'un délai de 3 mois à compter de sa désignation pour mener à bien sa mission. Les parties peuvent décider de proroger ce délai d'un commun accord. Aucune saisine du juge ne pourra avoir lieu avant son expiration, si ce n'est de l'accord exprès des deux parties. Celles-ci s'engagent à collaborer de bonne foi avec le médiateur. Le médiateur a pour mission d'assister les parties afin qu'elles règlent amiablement leur différend. Le médiateur entend à cette fin chaque partie, ainsi que toute personne dont il jugerait devoir recueillir les observations. Il peut solliciter la communication de tout document utile à sa mission. Le médiateur est tenu au secret.

En cas d'échec de la médiation, aucune des informations échangées entre les parties ne pourra être utilisées contre l'autre. La rémunération du médiateur est supportée à part égale par les deux parties.

En cas d'échec de la médiation, tout différend relatif aux présentes conditions sera tranché par le Tribunal de Commerce de GRENOBLE, même en cas de référé, d'appel en garantie ou de pluralité de défendeurs.

ARTICLE 19 – RENONCIATION

Le fait pour TRILOG de ne pas se prévaloir à un moment donné de l'une quelconque des clauses des présentes ne peut valoir renonciation à se prévaloir ultérieurement de ces mêmes clauses.

ARTICLE 20 - CLAUSES CONTRACTUELLES DE SOUS-TRAITANCE EN APPLICATION DU REGLEMENT EUROPEEN SUR LA PROTECTION DES DONNEES PERSONNELLES

20.1. OBJET

Les présentes clauses ont pour objet de définir les conditions dans lesquelles la société TRILOG, ci-après dénommée le "sous-traitant", s'engage à effectuer pour le compte de son Client, ci-après dénommé le "responsable de traitement", les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la règlementation en vigueur applicable au traitement des données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après "le règlement sur la protection des données).

Plus particulièrement, la société TRILOG met en œuvre les actions nécessaires à sa bonne application :

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

- Nomination d'un Délégué à la Protection des Données (DPO)
- Constitution du registre des traitements
- Cartographie des flux et des risques associés
- Mise en œuvre d'une procédure d'alerte en cas de compromission des données

TRILOG s'engage à coopérer et à fournir au Client, sur simple demande écrite adressée au siège social, l'ensemble des procédures permettant au Client de répondre à l'exercice des droits des personnes tels que définis par les articles 15 à 22 du règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016.

20.2. DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DE LA SOUS-TRAITANCE

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir tout matériel et prestations dans le domaine informatique.

Nature des opérations réalisées sur les données : déplacements et transfert de données,

Finalités du traitement : installation, réparation et maintenance de matériel et logiciels servant notamment à l'exploitation, au transfert et au stockage de données, formation des utilisateurs desdits matériels et logiciels,

Type de données à caractère personnel traitées : noms, prénoms, dates et lieux de naissance, adresses postales et courriels, coordonnées téléphoniques et informations médicales,

Type de personne concernées : clients, personnels du client, patients et fournisseurs du client

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes : liste et emplacement de données à transférer ou sauvegarder.

20.3. DUREE DU CONTRAT

Les présentes clauses s'appliquent durant toute la durée du contrat conclu entre la société TRILOG et son client.

Les présentes clauses seront reconduites dans les mêmes conditions que le contrat auquel elles sont attachées.

20.4. OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DE TRAITEMENT

TRILOG s'engage à :

1. Traiter les données uniquement pour les seules finalités faisant l'objet de la sous-traitance,

2. Traiter les données conformément aux instructions documentées du Client. Si la société TRILOG considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou toute autre disposition du droit de l'Union ou du droit des Etats membres relatives à la protection des données, elle en informe immédiatement le Client. En outre si TRILOG est tenue de procéder à un transfert de données vers un pays tiers ou une organisation internationale, en vertu du droit de l'union ou du droit de l'Etat membre auquel il est soumis, TRILOG doit informer le Client de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public,

3. Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat,

4. Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :

- s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,
- reçoivent la formation nécessaire en matière de protection des données à caractère personnel

5. Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données.

6. Sous-traitance

Le sous-traitant en la personne de TRILOG, peut faire appel à un autre sous-traitant (ci-après le "sous-traitant ultérieur") pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable de traitement dispose d'un délai minimum de 15 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

7. Droit d'information des personnes concernées

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

8. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

A cet effet, lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique au Client, sous réserve que ce dernier ait fourni au sous-traitant une adresse email valide.

9. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement dans un délai maximum de vingt-quatre (24) heures après en avoir pris connaissance, par l'envoi d'un message électronique, à l'adresse email fournie par le responsable de traitement. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

10. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement,

- les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique,

- une procédure visant à tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Toutes les autres mesures de sécurité relèvent de la seule responsabilité du Client.

12. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à détruire toutes les données à caractère personnel

13. Délégué à la protection des données

Le sous-traitant communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen de protection des données.

14. Registre des catégories d'activités de traitement

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

- Le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données;
- Les catégories de traitements effectués pour le compte du responsable du traitement;

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées.

- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :

. la pseudonymisation et le chiffrement des données à caractère personnel,
. des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement,
. des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique,
. une procédure visant à tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

15. Documentation

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

20.5. OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS-A-VIS DU SOUS-TRAITANT

Le responsable de traitement s'engage à :

- Fournir au sous-traitant les données visées au II des présentes clauses;

- Documenter par écrit toute instruction concernant le traitement des données par le sous-traitant;

- Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant;

- Superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

ARTICLE 21 - CONTRAT DE PRESTATION DE SAUVEGARDE AVEC HEBERGEMENT CERTIFIE HDS

TRILOG a mis en place une offre appelée KIWI BACKUP SANTE, ayant pour objet la sauvegarde externe et mutualisée de données à destination des professionnels du secteur de la santé.

Le Client de la société TRILOG ayant souscrit l'offre KIWI BACKUP SANTE s'engagent à respecter l'ensemble des dispositions du présent article qui vaut contrat de prestations de sauvegarde.

Le Client a choisi TRILOG pour la connaissance de son secteur d'activité parce que le logiciel de sauvegarde de la solution KIWI BACKUP SANTE ainsi que l'hébergement certifié HDS répondent aux obligations légales imposées par l'Asip Santé (Hébergement en France chez OVH Healthcare).

ARTICLE 21.1 – DEFINITIONS

Données de santé : Donnée, généralement à caractère personnel, liée à la santé physique et/ou psychique d'une personne physique identifiée ou pouvant être identifiée.

Hébergement HDS : Hébergement certifié données de santé, c'est-à-dire remplissant l'ensemble des dispositions légales et règlementaires applicables (notamment article L1111-8 du Code de la Santé Publique modifié par la loi n° 2016-41 du 26 janvier 2016 et article R111-9 et suivants dudit code issus du Décret n°2006-6 du 04.01.2006).

ARTICLE 21.2 – OBJET DU CONTRAT

Le présent contrat de prestation de sauvegarde de données avec hébergement certifié HDS a pour objet de compléter les articles 1 à 20 des présentes Conditions Générales de vente et de prestations, qui s'appliquent en l'état de plein droit, afin de prendre en compte l'ensemble des obligations liées à la sauvegarde de données de santé.

ARTICLE 21.3 - PROTECTION DES DONNEES RELATIVES A LA SANTE DES PERSONNES

21.3.1. PERIMETRE ET FINALITE DU SERVICE KIWI BACKUP SANTE

Les Données relatives à la santé étant des Données sensibles, leur traitement et leur collecte sont encadrés.

Le traitement de Données à caractère personnel effectué par KIWI BACKUP pour le compte de TRILOG et in fine, du Client a pour seule finalité la sauvegarde des Données de santé. La solution KIWI BACKUP SANTE permet la sauvegarde des Données de santé (tous types de Données, administratives, résultats d'examens etc.) qui bénéficient d'un Hébergement de Données de santé à caractère personnel au sens de l'article L. 1111-8 du Code de la santé publique. KIWI BACKUP et TRILOG s'engagent notamment à ne pas utiliser les données de santé hébergées par KIWI BACKUP et auxquelles TRILOG peut avoir accès pour les besoins du service pour des fins marketings, publicitaires, commerciales, statistiques ou tout autre ne correspondant pas à la finalité du traitement.

Les personnes destinataires de ces Données sont uniquement les Clients ainsi qu'éventuellement ses sous-traitants déclarés auprès des personnes concernées par les Données (Annexe).

Le service KIWI BACKUP SANTE ne permet en aucun cas un accès direct du patient aux Données de santé le concernant. Les seules personnes disposant d'un accès sont KIWI BACKUP, TRILOG et le Client.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

21.3.2. HEBERGEMENT DU SERVICE KIWI BACKUP SANTE

La société OVH, Société par actions simplifiée au capital de 10 069 020 € immatriculée au RCS de Lille Métropole sous le n° 424 761 419 00045 dont le siège social est situé 2 rue de Kellermann – BP 80157, 59100 ROUBAIX, a été sélectionnée par KIWI BACKUP comme un sous-traitant hébergeur conforme aux exigences réglementaires pour la prestation.

Cet hébergeur est certifié pour une prestation d'Hébergement d'applications fournies par les Clients et gérant des Données de santé à caractère personnel, via son offre "*Private Cloud OVH HEALTHCARE*".

21.3.3. PLAN DE REPRISE D'ACTIVITE (PRA)

KIWI BACKUP a mis en place un PRA qui pourra être activé en cas d'incident majeur sur la plateforme d'hébergement de données de santé.

Le PRA mis en place garantit la redondance des données sur un serveur HDS, hébergé dans un Data Center distinct du Data Center principal.

ARTICLE 21.4 – RESPONSABILITE DE L'EDITEUR

21.4.1. SECURITE DES DONNES

KIWI BACKUP s'engage à prendre toutes précautions utiles, au regard de la nature des Données et des risques présentés par le service de sauvegarde, pour préserver la sécurité des Données. Il s'engage notamment à assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité du logiciel de sauvegarde et des interfaces utilisateur et d'administration. En particulier, il s'engage à ce qu'en aucun cas des Données de santé ne transitent en clair sur les équipements qui sont sous sa responsabilité ou sur un réseau public.

KIWI BACKUP s'engage notamment à :

- Formaliser une politique de sécurité dont le champ d'application couvre le logiciel de sauvegarde et les interfaces utilisateur et d'administration, ainsi que les Données de santé ;
- Assurer la sécurité de l'architecture réseau ;
- Assurer la sécurité des postes de travail et des équipements à partir desquels son personnel, et toute personne autorisée par lui, accèdent au logiciel de sauvegarde et aux interfaces client et d'administration, ainsi qu'aux Données de santé ;
- Gérer finement les habilitations, l'identification, l'authentification et le contrôle d'accès de son personnel et des Utilisateurs au logiciel de sauvegarde et aux interfaces utilisateur et d'administration ;
- Contrôler l'utilisation des moyens d'authentification forte par les personnes habilitées à accéder à l'interface d'administration ;
- Assurer la traçabilité des accès et des opérations réalisées sur le logiciel de sauvegarde et l'interface d'administration, tant par son personnel que par les Utilisateurs ;
- Assurer la sécurité des communications et des transferts d'information ;
- Gérer les Incidents de sécurité sur son périmètre d'activité ;
- Sensibiliser et former son personnel à la sécurité des systèmes d'information ;
- Sensibiliser son personnel à la confidentialité et au respect du secret professionnel, et plus particulièrement concernant les Données de santé à caractère personnel déposées dans le cadre du service ;
- Sauvegarder les données de traçabilité des accès et des opérations réalisées sur le logiciel de sauvegarde et l'interface d'administration ;
- Mettre en œuvre un plan de continuité ou de reprise d'activité.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

21.4.2. GESTION DES INCIDENTS

KIWI BACKUP a mis en place une procédure de gestion des incidents et s'engage à notifier à TRILOG, qui informera le Client, toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

ARTICLE 21.5 – RESPONSABILITE DU PRESTATAIRE

21.5.1 SECURITE DES DONNES

TRILOG s'engage à prendre toutes précautions utiles, au regard de la nature des Données et des risques présentés par le service de sauvegarde, pour préserver la sécurité des Données. Il s'engage notamment à ce qu'en aucun cas des Données de santé ne transitent en clair sur les équipements qui sont sous sa responsabilité ou sur un réseau public.

TRILOG s'engage notamment à :

- Appliquer la politique de sécurité de KIWI BACKUP, dont le champ d'application couvre le logiciel de sauvegarde et les interfaces utilisateur et d'administration, ainsi que les Données de santé ;
- Assurer la sécurité des postes de travail et des équipements à partir desquels son personnel, et toute personne autorisée par lui, accèdent au logiciel de sauvegarde et aux interfaces client et d'administration, ainsi qu'aux Données de santé ;
- Gérer finement les habilitations, l'identification, l'authentification et le contrôle d'accès de son personnel et des Utilisateurs au logiciel de sauvegarde et aux interfaces utilisateur et d'administration ;
- Contrôler l'utilisation des moyens d'authentification forte par les personnes habilitées à accéder aux Données de santé ;
- Participer à la gestion des Incidents de sécurité sur son périmètre d'activité ;
- Sensibiliser et former son personnel à la sécurité des systèmes d'information ;
- Sensibiliser son personnel à la confidentialité et au respect du secret professionnel, et plus particulièrement concernant les Données de santé à caractère personnel déposées dans le cadre du service ;

21.5.2. GESTION DES INCIDENTS

Suite à une notification de KIWI BACKUP, TRILOG s'engage à informer le Client de toute violation de données à caractère personnel, et ce dans les meilleurs délais après en avoir pris connaissance.

21.5.3. RESPECT DE LA PSSI

TRILOG s'engage à respecter les principes fondateurs de la PSSI (Politique générale de sécurité des systèmes d'information de santé) de KIWI BACKUP et à se conformer aux référentiels techniques et aux guides associés. Il incombe à TRILOG de s'assurer que ses propres Clients et tout acteur intervenant dans le cadre du Service, gèrent les données de santé dans le respect de la PSSI.

ARTICLE 21.6 – RESPONSABILITE DU CLIENT

21.6.1. SECURITE DES DONNEES

Le Client s'engage, en sa qualité de responsable de traitement, à prendre toutes les mesures lui permettant d'être en conformité avec le Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des Données à caractère personnel et à la libre circulation de ces Données relatives à la protection des Données de santé et notamment lui permettant de recueillir le consentement de la personne concernée à l'Hébergement de ses Données de santé.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

TRILOG reporte expressément la couverture de certaines obligations légales et réglementaires liées à la sécurité sur le Client. Ainsi, les obligations suivantes relèvent exclusivement de la responsabilité du Client :

- Assurer la sécurité des postes de travail et des équipements à partir desquels son personnel, et toute personne autorisée par lui, accèdent au logiciel de sauvegarde, à l'interface utilisateur et, si TRILOG a communiqué l'accès au Client à l'interface d'administration ;
- Gérer finement les habilitations, l'identification, l'authentification et le contrôle d'accès de son personnel et des Utilisateurs au logiciel de sauvegarde, à l'interface utilisateur et à l'interface d'administration ;
- Contrôler l'utilisation des moyens d'authentification forte par les personnes habilitées à accéder aux Données de santé ;
- Gérer les Incidents de sécurité sur son périmètre d'activité ;
- Sensibiliser et former son personnel à la sécurité des systèmes d'information ;
- Sensibiliser son personnel à la confidentialité et au respect du secret professionnel, et plus particulièrement concernant les Données de santé à caractère personnel déposées dans le cadre du service.

21.6.2. GESTION DES INCIDENTS

Le Client s'engage à communiquer (par courriel) au Prestataire l'identité et les coordonnées d'un interlocuteur référent à joindre pour la gestion des incidents ayant une répercussion sur les données de santé sauvegardées dans le cadre du présent contrat.

ARTICLE 21.7 – AUDITABILITE

21.7.1. AUDIT A LA DEMANDE DU CLIENT

Le Client pourra, à fréquence raisonnable (au maximum une fois par an), réaliser ou faire réaliser par un tiers prestataire reconnu, un audit de la solution KIWI BACKUP SANTE dans les conditions ci-après.

Le Client notifie la demande d'audit à TRILOG par écrit avec délai de prévenance d'au moins 60 jours, en précisant, pour validation de TRILOG, la nature et le périmètre de l'audit souhaité ainsi que l'identité de toutes les personnes (y compris tiers prestataires auditeur) auxquelles le Client souhaite confier la réalisation de l'audit. TRILOG notifiera à son tour la demande auprès de KIWI BACKUP par écrit avec un délai de prévenance d'au moins 30 jours, en précisant, pour validation de KIWI BACKUP, la nature et le périmètre de l'audit souhaité ainsi que l'identité de toutes les personnes (y compris tiers prestataires auditeur) auxquelles le Client souhaite confier la réalisation de l'audit

KIWI BACKUP, tout comme TRILOG, se réservent le droit, pour motif légitime, de refuser la participation de certaines personnes et/ou tiers prestataires auditeurs à l'audit (notamment à des concurrents de KIWI BACKUP et/ou de TRILOG, des personnes en lien avec des concurrents de KIWI BACKUP et/ou de TRILOG, ou des personnes avec lesquelles un conflit d'intérêt avec KIWI BACKUP et/ou TRILOG est établi). Toute personne participant à l'audit s'engage au préalable et par écrit avec KIWI BACKUP et/ou TRILOG dans le cadre d'un accord de confidentialité.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Le périmètre d'audit doit être pertinent, et ne peut notamment porter que sur le service KIWI BACKUP SANTE fourni par TRILOG au Client en exécution du présent Contrat. En cas de visite sur site, il s'agit d'une visite d'une demi-journée, encadrée et supervisée par TRILOG, réalisée pendant les horaires habituels de fonctionnement du site de TRILOG. Au cours de la visite, un responsable de TRILOG est disponible pour répondre aux questions du Client sur l'organisation et les mesures de sécurité mises en œuvre. TRILOG a la possibilité de demander un appui par téléphone ou en présentiel à KIWI BACKUP. La visite est réalisée dans le respect des règles de sécurité de TRILOG, et ne doit pas perturber l'activité et le bon fonctionnement des services de TRILOG. En aucun cas, le Client ne pourra prétendre avoir accès à des sites et/ou informations sensibles de TRILOG et de KIWI BACKUP telles que données stratégiques, secrets de fabrique, éléments de propriété intellectuelle, données et informations d'autres clients, etc. que TRILOG et KIWI BACKUP se réservent le droit de garder confidentiels. Le Client s'engage à l'issue de l'audit, à réaliser ou à faire réaliser par le tiers prestataire en charge de la réalisation de l'audit, un rapport d'audit écrit, et à le communiquer à TRILOG qui le fera suivre à KIWI BACKUP. Le rapport d'audit est discuté contradictoirement.

21.7.2. DEMANDE DE RAPPORT D'AUDIT

Le Client pourra demander à TRILOG la communication des rapports d'audit ayant été réalisés par KIWI BACKUP auprès des organismes compétents.

21.7.3. CONFIDENTIALITE DES RAPPORTS D'AUDIT

Les rapports d'audit, leur contenu, et plus généralement toutes les informations divulguées dans le cadre de l'audit sont considérées comme strictement confidentielles, et ne peuvent sous aucun prétexte être divulgués à des tiers sans accord préalable, écrit et signé de TRILOG et de KIWI BACKUP.

ARTICLE 21.8– LISTE DES ANNEXES

- ANNEXE 1 – INFORMATIONS RELATIVES AUX FORMALITES PREALABLES AUPRES DE LA CNIL
- ANNEXE 2 – LISTE DES SOUS-TRAITANTS DE TRILOG
- ANNEXE 3 – PSSI de l'EDITEUR– Politique de Sécurité des Systèmes d'Information
- ANNEXE 4 – LETTRE D'ENGAGEMENT DE LA DIRECTION de KIWI BACKUP
- ANNEXE 5 – CERTIFICAT HDS OVH
- ANNEXE 6 – Certificat ISO 27001 de KIWI BACKUP
- ANNEXE 7 – Certificat HDS de KIWI BACKUP

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

ANNEXE 1 – INFORMATIONS RELATIVES AUX FORMALITES PREALABLES AUPRES DE LA CNIL

http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_professionnels_de_sante.pdf

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

ANNEXE 2 – LISTE DES SOUS-TRAITANTS DE TRILOG

(sur demande)

SMSI

Politique

Politique de Sécurité du Système d'Information

État Cycle de Vie : Publié

Identification du document	
Référence	SMSI_POL001
Version	V3.0
Classification	Interne

Assurez-vous d'utiliser la dernière version du document en consultant le site de référence.

Kiwi Backup
40 rue Victor Schoelcher
68200 MULHOUSE
Tél : 03 89 333 888

CYCLE DE VIE DU DOCUMENT

AUTEUR(S)

Fonction	Nom
Conseil	Patrick SCHOENIG
Chargée de projet	Céline THEVENET

RELECTEUR(S)

Fonction	Nom	Date
Chargée de projet	Céline THEVENET	06/05/2019
RSSI	Sébastien HEITZMANN	16/05/2019

Administrateur système	Morgan WERNER	16/05/2019
Chargée de projet	Céline THEVENET	17/07/2019
RSSI	Sébastien HEITZMANN	17/07/2019
Administrateur système	Morgan WERNER	17/07/2019

VALIDATION

Fonction	Nom	Date
RSSI	Sébastien HEITZMANN	17/07/2019
RSSI	Sébastien HEITZMANN	12/09/2019

HISTORIQUE DU DOCUMENT

Version	Date	Description	Détails
0.1	03/04/2019	Création du document et diffusion pour relecture, état « Pour commentaire »	P.S.
0.2	12/04/2019	Revue et ajustement lors des ateliers 10-11 avril 2019 et diffusion pour relecture (politique de mot de passe)	P.S.
0.3	06/05/2019	Relecture et amendement	CT
0.4	16/05/2019	Relecture par l'équipe	SH / MW / CT
0.5	24/05/2019	Ajout de l'échelle de besoin en traçabilité et diffusion pour relecture	P.S.
0.6	03/07/2019	Relecture et intégration points ISO 20000	SH / MW / CT
1.0	17/07/2019	Validation pour diffusion	SH
2.0	26/08/2019	Ajout référence loi I&L 2018 + décret 2019 dans paragraphe 14.1 et validation pour diffusion	CT/SH
2.1	10/09/2019	Intégration remarques suite à audit interne	CT
3.0	12/09/2019	Validation pour diffusion	SH

SOMMAIRE

1 Introduction

1.1 Préambule

La Politique de Sécurité du Système d'Information (PSSI) de Kiwi Backup vise à définir les règles de sécurité au sein de l'organisme que tout manager ou collaborateur se doit de connaitre et appliquer.
La PSSI est un document public accessible à l'ensemble des parties intéressées internes de Kiwi Backup et peut-être portée à la connaissance des parties intéressées externes lorsque la protection des actifs de l'entreprise le justifie ou encore lorsque l'entreprise doit attester de ses bonnes pratiques en matière de sécurité.

1.2 Objectifs et périmètre

En tant qu'Entreprise de Services du Numérique (ESN), Kiwi Backup est concernée par la sécurité de l'information à double titre : pour sa propre sécurité et aussi pour celle de ses clients.

La mise en œuvre de la sécurité du système d'information chez Kiwi Backup a pour **objectifs** :

- de préserver la **confidentialité** : garantir que les données ne sont accessibles qu'aux personnes autorisées
- de préserver **l'intégrité** : garantir que les données n'ont pas été altérées durant les traitements
- de préserver la **disponibilité** : garantir le maintien du bon fonctionnement de l'ensemble du SI et ainsi l'accès aux services et ressources
- de préserver la **traçabilité** : garantir l'accès aux données permettant de comprendre les modifications effectuées sur les données

Ces 4 objectifs s'appliquent pour les informations propres à Kiwi Backup mais également pour les informations de ses clients qui transitent par son SI ou dont elle a la responsabilité.

Les objectifs de sécurité du SMSI détaillés sont décrits dans le Manuel du SMSI [R4], chapitre 3.2.2.

Cette PSSI couvre le SI de Kiwi Backup qui est détaillé dans le Dossier d'Architecture Technique [R7] et définit dans les chartes d'utilisation des ressources informatiques [R2] et administrateur du SI de Kiwi Backup [R3] comme « le système de traitement automatisé de l'entreprise, associé à des moyens techniques, qui fournit et distribue l'information ».

Le SI de Kiwi Backup est composé de 2 sous-ensembles :

- Les éléments de SI physiquement installés chez l'hébergeur de Kiwi Backup, et qui relèvent d'un contrat de service avec le fournisseur
- Les éléments de SI physiquement installés chez Kiwi Backup

Elle s'applique :

- A l'ensemble des collaborateurs de Kiwi Backup,
- Aux personnels temporaires (stagiaires, alternants et intérimaires),

- Aux tierces parties travaillant pour l'Entreprise,
- Et de manière plus générale, à toute personne ayant accès au système d'information de l'Entreprise.

Cette politique peut aussi s'appliquer aux collaborateurs de Kiwi Backup effectuant des missions chez un client, selon les termes précisés dans la charte [R2] : « Les salariés de l'Entreprise intervenant chez les clients de l'Entreprise ou ses partenaires devront également se conformer aux usages et directives en vigueur chez chaque client ou partenaire à la condition qu'ils leur soient communiqués. En l'absence de communication, les salariés devront appliquer les présentes règles au périmètre du client. »

1.3 Propriétaire et approbateur

Cette politique est sous la responsabilité du RSSI de Kiwi Backup. Elle est soumise à l'approbation de la direction de Kiwi Backup.

La PSSI fait référence aux normes ISO 27001:2013, ISO 27002:2013, ISO 20000 et ISO 27018. Elle est mise à jour annuellement en accord avec le comité de sécurité de l'Entreprise.

1.4 Portée, limites et exclusions

Cette politique de sécurité doit être appliquée à l'ensemble du SI et des collaborateurs de Kiwi Backup. Toute exception doit faire l'objet d'une dérogation écrite et validée par le RSSI.

1.5 Entrée en vigueur et mesures transitoires

Cette politique entre en vigueur dès son approbation.

1.6 Documents associés

TITRE	REFERENCE	VERSION
[R1] Règlement intérieur de Kiwi Backup		
[R2] Charte d'utilisation des ressources informatiques de Kiwi Backup	SMSI_CHA001	Publiée
[R3] Charte Administrateur SI de Kiwi Backup	SMSI_CHA002	Publiée
[R4] Manuel du SMSI	SMSI_GUI001	Publiée
[R5] Rôles et responsabilités des acteurs	SMSI_ORG001	Publiée
[R6] Procédure de gestion des mots de passe	SMSI_PRO015	Publiée
[R7] DAT Dossier d'Architecture Technique	DT_GUI005	Publiée
[R8] SMSI Politique de sécurité physique et environnementale	SMSI_POL002	Publiée
[R9] Procédure d'installation des nouvelles machines de production	SMSI_PRO008	Publiée
[R10] Procédure de journalisation	SMSI_ PRO006	Publiée
[R11] Procédure de gestion du Bastion	SMSI_PRO005	Publiée
[R12] Procédure de gestion du télétravail	SMSI_PRO018	Publiée
[R13] Procédure de gestion des vulnérabilités	SMSI_PRO016	Publiée
[R14] Support et restauration de données	SMSI_PRO010	Publiée

[R15] Procédure de gestion des changements	SMSI_PRO017	Publiée
[R16] Politique de conception et de transition de services nouveaux ou modifiés	SMSI_POL003	Publiée
[R17] Procédure de gestion des incidents de sécurité	SMSI_PRO002	Publiée
[R18] Plan de continuité d'activité	SMSI_PCA001	Publiée
[R19] Procédure de gestion des entrées, sorties et changements	SMSI_PRO014	Publiée
[R20] Procédure de recrutement Kiwi Backup	SMSI_PRO013	Publiée
[R21] Inventaire des actifs	DT_TAB003	Publiée
[R22] Plan de traitement des risques	SMSI_ADR002	Publiée
[R23] Procédure de gestion documentaire	SMSI_PRO001	Publiée
[R24] Liste des habilitations	DT_TAB002	Publiée
[R25] Registre des fournisseurs-sous-traitants	SMSI_TAB008	Publiée

1.7 Terminologie

1.7.1 Définitions

TERME DE LANGAGE	DEFINITION
Sécurité de l'information	Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information (ISO 27000, 2.19).
Bien essentiel ou actif principal	Identifie un processus métier, une activité ou une information que l'organisation souhaite protéger.
Actif support	Identifie une personne ou un équipement que l'organisation souhaite protéger, cet actif vient en support d'un ou plusieurs actifs principaux.
Entreprise ou Kiwi Backup	Dans le présent document les termes « Entreprise » et « Kiwi Backup » sont utilisés indifféremment pour nommer la société Kiwi Backup.
Appareils mobiles	Appareil portatif muni d'un système d'exploitation et d'applications (smartphones, tablettes…). Les ordinateurs portables ne sont pas considérés ici comme des appareils mobiles mais comme des postes de travail.
Télétravail	Le télétravail désigne toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur ou d'un client est effectué par un salarié depuis son domicile de façon régulière ou occasionnelle en utilisant les technologies de l'information et de la communication.
Bastion	Un bastion est un élément du réseau informatique qui fournit un point d'entrée et/ou de sortie unique vers un réseau externe (internet par exemple).
Projet / Livraison	L'unité de gestion de projet définie chez Kiwi Backup est la livraison. Celle-ci est gérée comme un projet à part entière depuis la définition du besoin jusqu'à la livraison en production et sa vérification.

1.7.2 Abréviations

ABREVIATION	SIGNIFICATION
PSSI	Politique de Sécurité du Système d'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information
DT	Directeur / Direction Technique
DRH	Directeur / Direction des Ressources Humaines (rôle)
RSG	Responsable des Services Généraux (rôle)
SMSI	Système de Management de la Sécurité des Systèmes d'Information
RGPD	Règlement Général européen sur la Protection des Données personnelles
DPD (DPO)	Délégué à la Protection des Données (Data Protection Officer)
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
RGS	Référentiel Général de Sécurité publié par l'ANSSI et décrivant entre autres la cryptographie
OWASP	Open Web Application Security Project
COSEC	Comité de sécurité
CAB	Change Advisory Board

2 Rôles et responsabilités [A.6.1]

L'ensemble des rôles et responsabilités est détaillé dans le document d'organisation Rôles et responsabilités des acteurs [R5].

2.1 RSSI

Il a en charge le pilotage de la sécurité du système d'information de Kiwi Backup en collaboration avec l'équipe technique, le responsable des services généraux, les ressources humaines et le service juridique.

Cela implique la description et la mise à jour dans le temps de cette politique de sécurité.

Il est le représentant de Kiwi Backup auprès des autorités, partenaires, fournisseurs et clients en matière de sécurité de l'information.

2.2 Comité de sécurité - COSEC

Le comité de sécurité est en charge :

- De s'assurer du maintien à jour de cette politique en accord avec l'évolution des besoins, des risques et des évolutions technologiques,
- De valider les politiques de sécurité déclinant cette PSSI,
- De suivre les demandes de dérogation à cette politique et aux directives et procédures associées.
- De conseiller le DT lors de la planification de changements impactant la sécurité du service, tel que décrit dans la politique de conception et transition des services nouveaux ou modifiés [R16].

Membres permanents :

- Directeur technique, RSSI
- Administrateur système, Support technique
- DPO

Invités sur demande :

- Direction
- Responsable Juridique
- Responsable des Ressources Humaines
- Directrice commerciale
- Service communication

3 Echelles des besoins de sécurité [A.8.2]

Le niveau de protection des informations traitées par un système d'information doit être proportionnel aux besoins de sécurité des biens essentiels qu'elles supportent.

La classification de l'information permet de déterminer les mesures de sécurité nécessaires à leur protection et est utilisée pour définir les besoins et priorités en matière de sécurité de l'information.

Les besoins primordiaux portent sur l'intégrité et la confidentialité. La disponibilité est secondaire par rapport à l'intégrité et la confidentialité.

3.1 Besoins en Disponibilité

Niveau de sensibilité	Définition
Plus de 72h	Le bien essentiel peut être indisponible plus de 72h
Entre 24 et 72h	Le bien essentiel doit être disponible dans les 72h
Niveau de sensibilité	**Définition**
Entre 4 et 24h	Le bien essentiel doit être disponible dans les 24h

3.2 Besoins en Intégrité

Niveau de sensibilité	Définition
Négligeable	Le bien essentiel peut ne pas être intègre
Détectable	Le bien essentiel peut ne pas être intègre si l'altération est identifiée
Maîtrisé	Le bien essentiel peut ne pas être intègre si l'altération est identifiée et l'intégrité du bien essentiel retrouvée
Intègre	Le bien essentiel doit être rigoureusement intègre

3.3 Besoins en Confidentialité

Niveau de sensibilité	Définition
Public	Informations qui peuvent être accessibles au public sans conséquence pour l'Entreprise (exemple : Site Internet de l'Entreprise). Une information doit volontairement être classifiée comme publique.
Interne	Informations ayant vocation à rester au sein de l'Entreprise (exemple : procédure qualité). La diffusion de ces informations à un destinataire extérieur à l'Entreprise doit être validée par le propriétaire de l'information ou sa hiérarchie. Ces informations sont librement accessibles aux utilisateurs de l'Entreprise et aux personnes externes autorisées. **Une information est classifiée interne par défaut.**
Confidentiel	Informations dont la divulgation à l'extérieur des groupes de personnes internes ou externes autorisés peut avoir des conséquences importantes pour l'Entreprise. Une information doit volontairement être classifiée au niveau de sensibilité « confidentiel ». Son propriétaire doit désigner clairement les groupes de personnes autorisées à y accéder et les informer des restrictions d'accès sur les informations.
Critique	Informations dont la divulgation à des personnes qui n'en sont pas nommément destinataires peut avoir un impact grave pour l'Entreprise (exemple : mot de passe, informations clients, information relevant du délit d'initié). Une information doit volontairement être classifiée au niveau de sensibilité « critique ». Son propriétaire doit désigner clairement les groupes de personnes autorisées à y accéder et les informer des restrictions d'accès sur les informations.

Par défaut, l'information collectée, traitée, stockée et diffusée par le système d'information de Kiwi Backup est considérée de niveau « interne ».

3.4 Besoins en Traçabilité

Niveau de sensibilité	Définition
Indicatif	Les traces peuvent être mises en œuvre et un traitement peut être nécessaire pour les rendre exploitables.
Auditable	Les traces doivent exister et peuvent être rendues disponibles dans un délai court.
Interne	Les traces doivent être formalisées, exploitables systématiquement, rapidement et opposables en interne.
Niveau de sensibilité	**Définition**
Légale	Les traces doivent être formalisées, exploitables systématiquement, rapidement et acceptables par un tribunal.

4 Sécurité liée aux collaborateurs [A.7]

4.1 Avant l'embauche

4.1.1 La sécurité de l'information dans les descriptions de poste

Lorsque cela est justifié, les rôles et responsabilités en matière de sécurité de l'information des collaborateurs sont formalisés dans leur fiche de poste. Des engagements de confidentialité sont signés par les collaborateurs en adéquation avec le niveau de sensibilité des informations auxquelles ils ont accès.

4.1.2 Sélection

En cas de besoin, les ressources humaines de Kiwi Backup mettent en place un processus de vérification des informations des candidats en accord avec la loi et la réglementation.

4.1.3 Accès au SI de Kiwi Backup

La procédure de gestion des entrées, sorties et changements [R19] s'assure que les nouveaux arrivants se voient attribuer des droits d'accès appropriés à leur fonction.

Les droits d'accès sont attribués suite à une demande formelle et approuvée par la hiérarchie via un ticket utilisant le template changement_RH. L'approbation est faite par le niveau hiérarchique approprié qui s'assure que les droits d'accès demandés correspondent bien à la fonction du nouvel arrivant.

Les droits d'accès attribués à des personnels temporaires ou externes doivent avoir une date d'expiration au moins équivalente à la fin du contrat.

La procédure de recrutement Kiwi Backup [R20] décrit les contrôles effectués préalablement à une embauche.

4.2 Pendant la durée du contrat

4.2.1 Sensibilisation et formation en matière de sécurité de l'information

Kiwi Backup met en place un programme de sensibilisation de l'ensemble des collaborateurs de l'Entreprise, ainsi que des personnels externes.

Ce programme sensibilise les utilisateurs manipulant les données à caractère personnel aux risques, aux mesures à appliquer et aux conséquences potentielles en cas de manquement.

Les collaborateurs de Kiwi Backup assumant des rôles et responsabilités en matière de sécurité de l'information bénéficient d'un programme de formation adéquat.

4.2.2 Processus disciplinaire

La charte d'utilisation des ressources informatiques [R2] établit les règles en matière de sanctions disciplinaires pour un collaborateur ne respectant pas les règles d'utilisation du SI.

4.2.3 Changement des droits d'accès

En cas de changement de fonction d'un collaborateur ou d'un utilisateur tiers, les droits d'accès au SI sont modifiés en conséquence.

Les responsables hiérarchiques concernés en effectuent la demande via le processus de gestion des entrées, sorties et changements [R19].

4.2.4 Utilisation des smartphones

Les collaborateurs sont autorisés à utiliser les téléphones fournis par Kiwi Backup dans le respect des règles d'utilisation définies dans la charte d'utilisation des ressources informatiques [R2].

4.3 A la fin du contrat de travail

4.3.1 Retrait des droits d'accès

Le processus de gestion des accès s'assure que les collaborateurs et les utilisateurs tiers quittant l'Entreprise se voient retirer leurs droits d'accès en temps opportun.

Les ressources humaines ont la responsabilité de notifier les départs conformément à la procédure de gestion des entrées, sorties et changements [R19] via un ticket utilisant le template changement_RH.

4.3.2 Retour du matériel

Il est du devoir de l'ensemble des collaborateurs et utilisateurs tiers de ramener au Responsable des Services Généraux la totalité des biens appartenant à Kiwi Backup, y compris le poste de travail, le smartphone, le badge d'accès, les données et les documents couverts par les règles de la propriété intellectuelle.

Le supérieur hiérarchique est responsable du bon retour des biens à Kiwi Backup et que les données présentes sur le matériel informatique retourné sont correctement sauvegardées si nécessaire.

La DT doit s'assurer que toutes les données sensibles ont bien été supprimées et les logiciels sous licence désinstallés ou écrasés de façon sécurisée, avant la mise au rebut ou la réutilisation du matériel.

5 Mobilité et télétravail [A.6.2]

5.1 Appareils mobiles

Seuls les appareils mobiles professionnels fournis par Kiwi Backup sont autorisés à se connecter au SI de l'Entreprise.

Des smartphones et tablettes sont mis à disposition des collaborateurs par les moyens généraux selon les besoins et les fonctions des collaborateurs après demande et validation de la hiérarchie.

L'administrateur système gèrent un inventaire des appareils mobiles.

Les collaborateurs sont autorisés à utiliser les téléphones fournis par Kiwi Backup dans le respect des règles d'utilisation définies dans la charte d'utilisation des ressources informatiques [R2].

Les collaborateurs doivent mettre à jour leurs smartphones dès que des mises à jour sont mises à disposition par l'opérateur téléphonique ou le fabriquant.

Les collaborateurs doivent activer l'écran de verrouillage et la fonction mot de passe dans les paramètres de leurs smartphones.

Les collaborateurs doivent sauvegarder leurs données importantes sur l'espace dédié Seafile de Kiwi Backup. Les collaborateurs et les utilisateurs tiers doivent ramener aux services généraux les appareils mobiles appartenant à Kiwi Backup lors de leur départ de l'Entreprise. Le supérieur hiérarchique est responsable de s'assurer que les biens sont retournés à Kiwi Backup et que les données présentes sur le matériel informatique retourné sont correctement sauvegardées si nécessaire.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Conformément aux bonnes pratiques en matière de gestion des matériels et supports amovibles, la DT doit s'assurer que toutes les données sensibles et les logiciels sous licences ont bien été effacés de façon sécurisée, avant la mise au rebut ou la réutilisation du matériel.

5.2 Télétravail

Le télétravail qui implique le fait de travailler de manière récurrente depuis chez soi n'est autorisé par l'Entreprise que dans des cas exceptionnels et fait l'objet de la signature d'un avenant au contrat de travail entre Kiwi Backup et le collaborateur.

En cas de télétravail, le collaborateur et Kiwi Backup s'assurent du bon fonctionnement de la ligne de téléphonie sur IP professionnelle au domicile du collaborateur si nécessaire.

L'ensemble du matériel informatique nécessaire à la réalisation de la mission dans le cadre du télétravail récurrent est fourni par la DT de l'Entreprise.

L'accès au SI de Kiwi Backup se fait via des accès sécurisés identiques aux conditions d'accès utilisées depuis les locaux de l'entreprise.

Son ordinateur professionnel accédant au SI de l'Entreprise, le collaborateur doit respecter l'ensemble des règles de sécurité et d'utilisation du SI qui s'imposent à lui en cas de travail depuis les locaux de Kiwi Backup.

Les mesures détaillées s'appliquant au télétravail sont détaillées dans la procédure de gestion du télétravail [R12].

6 Gestion des actifs [A.8]

6.1 Actifs

6.1.1 Gestion des actifs

Les actifs support sont identifiés dans l'inventaire des actifs [R21] par l'administrateur système et un propriétaire doit être affecté à chacun d'eux.

Le propriétaire de l'actif est responsable de l'actif durant son cycle de vie et de la mise en place des mesures de sécurité adéquates. La gestion d'un actif peut être déléguée au service compétent.

La personne en charge de la gestion de l'actif est responsable de l'état d'inventaire et doit signaler au RSSI tout événement (faille, risque, incident) pouvant compromettre la sécurité de cet actif.

Tout actif critique ou confidentiel, doit être stocké dans un espace sécurisé.

L'utilisation des dossiers partagés internes ou confidentiels, selon les cas est obligatoire pour tout document produit dans le cadre de l'activité de Kiwi Backup.

Tout actif doit être utilisé conformément à son objet et selon son niveau de classification.

Tout actif mis à disposition du personnel interne ou des tiers doit être restitué en fin de mission ou de contrat.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

6.1.2 Niveaux de classification des actifs

Niveau de classification	Définition
Interne	Actif librement accessible à toute personne interne à l'entreprise (ex : imprimante). L'utilisation de l'actif et sa sortie éventuelle de l'entreprise doit respecter les règles définies dans la charte d'utilisation des ressources informatiques [R2]. **Un actif est classifié interne par défaut.**
Confidentiel	Actif permettant un accès à des informations classifiées confidentielles, sensibles ou de santé (ex : administration de la plateforme Kiwi Santé). Ces actifs bénéficient de mesures de sécurité renforcées (stockage en zone 3 sécurisée, habilitations limitées, journalisation des accès dès que possible). Un actif doit volontairement être classifiée au niveau de sensibilité « confidentiel ». Son propriétaire doit désigner clairement les groupes de personnes autorisées à y accéder et les informer des restrictions d'accès.
Critique	Actif permettant un accès à des informations classifiées critiques. (exemple : mot de passe administrateur, informations clients, information relevant du délit d'initié). Ces actifs bénéficient de mesures de sécurité renforcées (idem confidentiel, redondance) Un actif doit volontairement être classifié au niveau de sensibilité « critique ». Son propriétaire doit désigner clairement les groupes de personnes autorisées à y accéder et les informer des restrictions d'accès en vigueur.

6.2 Matériels

Les matériels constituant la plateforme Kiwi Santé sont physiquement hébergés chez l'hébergeur de Kiwi Backup et leur sécurité est assurée par celui-ci (conformément à sa certification iso 27001), notamment pour les aspects physiques, réseau, électrique et de maintenance.

L'ensemble du matériel constituant l'infrastructure du SI de Kiwi Backup est placé dans les salles informatiques et les locaux techniques dont les accès sont gérés de façon sécurisée.

Les salles informatiques et les locaux techniques font l'objet de mesure de limitation des risques de menaces physiques et environnementales potentielles conformément au plan de traitement des risques [R22].

L'ensemble du matériel constituant l'infrastructure du SI de Kiwi Backup est maintenu en accord avec les spécifications des fournisseurs.

Toute sortie de matériel des salles informatiques et des locaux techniques doit être autorisée par le DT et faire l'objet d'un enregistrement.

Du fait de leurs fonctions, certains collaborateurs de Kiwi Backup sont amenés à sortir des actifs de l'entreprise (PC portables, tablettes, smartphones, supports amovibles et documents papier). Ces actifs sont sous la surveillance de leurs propriétaires lorsqu'ils sont en dehors des locaux. Ils doivent assurer la sécurité physique de ces appareils en les gardant à portée de vue ou dans des endroits sécuritaires dont les accès sont contrôlés.

Les ordinateurs portables doivent être attachés avec le câble fournit à cet effet par la DT lorsqu'ils sont utilisés sur des salons ou événements extérieurs.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Les collaborateurs doivent respecter l'ensemble des règles émises par Kiwi Backup, notamment en matière d'appareils mobiles. Les règles sont énoncées dans la Charte d'utilisation des ressources informatiques [R2].

Les collaborateurs doivent veiller à ne pas laisser en libre accès de l'information sensible (niveaux de sensibilité « confidentiel » ou « critique ») sous format papier ou sur un support d'audit électronique lorsqu'ils quittent leur bureau. Il convient de la stocker dans un espace sécurisé.

Les collaborateurs doivent veiller à ne pas laisser leur poste de travail sans surveillance et doivent verrouiller leurs sessions de travail en cas d'absence.

6.3 Supports

Aucun support d'archivage ou de sauvegarde n'est autorisé pour les données de santé, confidentielles ou critiques et aucune donnée de santé, confidentielle ou critique ne doit être enregistrée sur un support amovible.

Concernant les autres données, l'archivage et la sauvegarde se font exclusivement par le biais du logiciel de sauvegarde Kiwi Backup, ainsi que par l'historisation de l'outil de partage de documents interne Seafile.

Lors de la mise au rebut des supports ou avant leur réutilisation, toutes les données sensibles et les logiciels sous licences sont effacés de façon sécurisée.

Dans l'éventualité où des supports seraient utilisés à l'avenir, le transport de ceux-ci sera effectué par des prestataires de confiance ayant signé un contrat avec Kiwi Backup.Le support sera alors placé dans un emballage assurant sa protection pendant le transport.
Lors de la remise d'un support amovible à un transporteur, un bon de transport sera complété avec l'origine et la destination.
Le destinataire devra signer le bon de transport à l'arrivée.

6.4 Information

Toute information doit être classifiée (publique, interne, confidentielle, critique) par son propriétaire et protégée conformément à son caractère sensible.
Conformément à l'échelle des besoins, une information est classifiée interne par défaut.
Une attention particulière est apportée pour les niveaux critique et confidentiel, avec un marquage facilement reconnaissable, conformément à la procédure de gestion documentaire [R23].

7 Gestion des accès [A.9]

Tous les utilisateurs du SI de Kiwi Backup sont identifiés par un identifiant unique et personnel.

Les comptes génériques ne sont pas autorisés.

7.1 Modes d'authentification

7.1.1 Authentification forte

L'authentification forte est une méthode utilisant deux facteurs d'authentification différents pour authentifier un utilisateur.

Cette méthode doit être utilisée autant que possible, notamment pour les informations classées confidentielles ou critiques selon l'échelle de classification de l'information.

7.1.2 Authentification par mot de passe

Lorsque l'authentification forte n'est pas utilisée, l'authentification des utilisateurs doit se faire par un mot de passe conformément aux règles définies par Kiwi Backup dans la Procédure de gestion des mots de passe
[R6].

Les utilisateurs ont la responsabilité de garder leurs mots de passe confidentiels.

7.2 Gestion des droits d'accès

7.2.1 Droits d'accès

Les droits d'accès physiques et logiques sont attribués selon la fonction de l'utilisateur, ses besoins dans le cadre de ses fonctions (besoin d'en connaître) et la classification de l'information.

Ils sont attribués au travers de la procédure des entrées, sorties et changements [R19] après validation de la hiérarchie.

7.2.2 Séparation des tâches

L'attribution des droits d'accès doit prendre en compte la séparation des tâches incompatibles pour limiter les risques de mauvais usages.

7.2.3 Revue des droits d'accès

Une revue de l'ensemble des droits d'accès est menée semestriellement.

7.2.4 Contrôle d'accès physique au SI

L'accès physiques aux salles informatiques et aux locaux techniques est limité aux collaborateurs habilités. Ces locaux sont protégés par un système de contrôle d'accès physique.

7.3 Gestion des tierces parties [A.15]

7.3.1 Accès aux installations informatiques de Kiwi Backup

L'accès physique aux installations informatiques de Kiwi Backup par une tierce partie doit faire l'objet d'une demande validée par le RSSI, ces interventions sont tracées dans un registre (classeur permettant de stocker les bons d'intervention). Toute personne extérieure à Kiwi Backup est accompagnée par le RSSI ou un membre de son équipe lors de son intervention dans les locaux techniques.

Le matériel informatique d'une tierce partie ne doit pas être connecté directement sur le réseau de Kiwi Backup. Si l'accès au réseau de Kiwi Backup est requis par une tierce partie, elle doit utiliser du matériel de Kiwi Backup ou son matériel doit être placé dans une partie dédiée de l'infrastructure avec les mesures de sécurité nécessaires.

7.3.2 Accès distant au SI de Kiwi Backup par une tierce partie

L'accès distant au SI de Kiwi Backup par une tierce partie doit faire l'objet d'une étude de sécurité menée par le RSSI. La liste des accès distants et interconnexions doit être tenue à jour par le RSSI.

7.3.3 Utilisation de services en ligne

Seuls les services Cloud validés par le RSSI sont autorisés. En cas de besoin, une étude de sécurité est menée par le RSSI.

7.3.4 Clauses de sécurité dans les contrats avec des tierces parties

Les accords avec des tiers donnant accès au SI de Kiwi Backup incluent les exigences de sécurité et sont formalisés dans un document contractuel après accord de la direction de Kiwi Backup. L'accord doit être en place avant la fourniture de l'accès.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Les accords avec des sous-traitants s'appuient sur des contrats types incluant les clauses de sécurité nécessaires.

Les accords avec des fournisseurs de services informatiques donnent lieu à une revue des contrats des fournisseurs pour valider la prise en compte des exigences de sécurité de Kiwi Backup et, si nécessaire, ajouter les clauses manquantes.

7.3.5 Surveillance et revues des services des fournisseurs

Conformément aux accords conclus, Kiwi Backup s'assure par des revues ou des audits que la prestation de services assurée par le fournisseur est conforme aux attentes en matière de sécurité de l'information.

7.3.6 Surveillance et revues par des clients

Conformément aux accords conclus dans le cadre d'une prestation services, Kiwi Backup peut faire l'objet de revues ou audits par des clients ou une société tierce agissant pour leur compte afin de s'assurer de sa conformité aux attentes en matière de sécurité de l'information et de protection des données personnelles.

8 Sécurité physique et environnementale [A.11]

La sécurité physique des locaux est sous la responsabilité du RSG et inclut les systèmes de contrôles d'accès, de détection d'intrusion, de détection et de prévention incendie.

Le travail dans les zones sécurisées est sous la responsabilité du RSSI pour les salles informatiques et les locaux techniques.

Le document Politique de sécurité physique et environnementale [R8] décrit l'ensemble des mesures prises en terme de zonage des locaux, de contrôle d'accès pour chaque zone définie et de protection contre les menaces extérieurs. Il décrit en outre les obligations afférentes du RSG et du RSSI.

9 Sécurité dans les opérations [A.12, A.13]

9.1 Procédures de gestion de la sécurité

Les administrateurs du SI de Kiwi Backup sont responsables de la documentation des procédures d'exploitation, de leurs mises à jour et de leur diffusion aux personnes concernées après validation du DT.
Ces procédures doivent traduire les règles de sécurité définies dans cette PSSI en mesures opérationnelles.

La documentation doit être mise à jour régulièrement, afin d'être conforme à la réalité technique et organisationnelle de Kiwi Backup.

9.2 Protection du périmètre réseau

Kiwi Backup met en œuvre les moyens nécessaires au respect des besoins de la qualité de service et au maintien de la sécurité de son réseau (filtrage des flux, proxy, IDS/IPS...) ou les contractualise dans les contrats de service avec ses partenaires.

Toute interface entre le réseau de Kiwi Backup et des réseaux externes est protégée par un pare-feu contrôlant les flux entrants et sortants.

9.3 Cloisonnement des réseaux

Le réseau de Kiwi Backup est cloisonné en domaines conformément au Dossier d'Architecture Technique [R7] et aux besoins de sécurité des informations transitant par ces domaines.

L'accès entre les différents domaines est contrôlé au niveau du périmètre en utilisant une passerelle adéquate et dont l'efficacité prouvée correspond aux prérequis de Kiwi Backup en matière de sécurité de l'information conformément à la procédure d'installation des nouvelles machines de production [R9] et à la procédure de gestion du Bastion [R11].

9.4 Comptes à droits d'accès privilégiés

L'attribution et l'utilisation de comptes à privilèges élevés est restreinte.

Les privilèges associés aux comptes d'administration sont répertoriés dans la liste des habilitations [R24] et les droits privilégiés ne sont attribués qu'à des utilisateurs dont la fonction a été définie comme nécessitant ces accès.
Ils sont attribués au travers de la procédure des entrées, sorties et changements [R19] après validation de la hiérarchie.

Les comptes à privilèges élevés doivent être associés à un identifiant utilisateur unique.
Les actions des comptes à privilèges élevés sont enregistrées conformément à la procédure de journalisation [R10].
L'authentification des utilisateurs à privilèges doit se faire par une méthode d'authentification forte conformément aux règles définies par Kiwi Backup dans la Procédure de gestion des mots de passe [R6].

9.5 Comptes par défaut

Les comptes par défaut non indispensables au fonctionnement du système doivent être supprimés ou désactivés dès la fin de l'installation ou du déploiement du système. Des comptes dédiés doivent être créés pour les tâches d'administration.

Les comptes par défaut indispensables au fonctionnement du système ou qui ne peuvent pas être supprimés ou désactivés doivent se voir attribuer un nouveau mot de passe et doivent être gérés comme des comptes à privilèges élevés.

9.6 Sécurité de la messagerie électronique

L'information transitant par la messagerie électronique doit être protégée.
L'accès à la messagerie est contrôlé et les mesures nécessaires sont prises pour la disponibilité, ainsi que la fiabilité du service.

Les règles d'utilisation de la messagerie sont formalisées dans la charte d'utilisation des ressources informatiques [R2].

9.7 Accès à distance au SI

Les accès au SI Kiwi Backup depuis internet sont sécurisées. Les seules interfaces vers le SI sont des accès HTTPS ou SSH via le bastion. Ces accès utilisent des communications chiffrées et utilisent une authentification forte.

Les accès distants aux éléments sensibles sont filtrés par IP.

Ces accès sont attribués au travers de la procédure des entrées, sorties et changements [R19] après validation de la hiérarchie et du RSSI.

Les mesures détaillées à prendre dans le cadre du télétravail sont explicitées dans la procédure de gestion du télétravail [R12].

9.8 Protection contre les logiciels malveillants

Kiwi Backup met en place des logiciels anti-virus sur l'ensemble des machines Windows. Les mises à jour de ces logiciels sont propagées automatiquement sur les postes de travail et les serveurs.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Un logiciel anti-virus est utilisé pour contrôler les messages électroniques.

Les alertes antivirales sont traitées dans le cadre de la gestion des incidents de sécurité [R17].

9.9 Gestion des vulnérabilités techniques

Kiwi Backup réalise une veille des vulnérabilités pour les systèmes composants son SI et applique les mesures nécessaires à la limitation des risques après analyse par le DT et le RSSI.

Kiwi Backup maintient une veille active via l'appartenance à des groupes d'experts et des lettres de diffusion traitant de ce sujet. Et effectue ensuite une analyse de la gravité des vulnérabilités et de leur impact potentiel sur le SI afin de décider des mesures à prendre. Il peut s'agir du déploiement d'un correctif si celui-ci a été développé par l'éditeur, de la mise en place d'une mesure compensatoire, ou de l'acceptation du risque si l'organisation est peu exposée ou déjà couverte par des mesures de sécurité en place.

Les systèmes et logiciels font l'objet de mises à jour régulières via des patchs de sécurité.

Les mesures de gestion des vulnérabilités sont détaillées dans la procédure de gestion des vulnérabilités [R13].

9.10 Utilisation de moyens de chiffrement [A.10]

Lorsque cela est nécessaire, des moyens de chiffrement sont définis et mis en œuvre pour protéger la sécurité de l'information en accord avec les niveaux de classification, conformément au DAT Dossier d'Architecture technique [R7].

Kiwi Backup ne développe pas de logiciel ou de librairie de chiffrement, mais utilise des outils standards du marché après analyse des risques par le DT et le RSSI.

Les mécanismes et protocoles utilisées sont conformes aux recommandations de l'ANSSI et du RGS.

9.11 Sauvegarde et reprise d'activité

9.11.1 Rôles et responsabilités

Les propriétaires de l'information ont la responsabilité de définir leurs besoins de sauvegarde et de restauration en accord avec la DT, y compris la fréquence des tests.

9.11.2 Exigences minimales concernant les sauvegardes

En cas d'absence d'exigences des propriétaires de l'information, un niveau de sauvegarde minimum est appliqué :

Fréquence	Type	Durée de rétention
Journalière	Incrémentale	90 jours

9.11.3 Vérification des sauvegardes

Des contrôles systématiques sont mis en place pour valider que les tâches liées à la sauvegarde se sont réalisées avec succès.

9.11.4 Tests des sauvegardes et restauration de données

La DT doit mener des tests de lecture et de restauration des données sur la base d'échantillons.

En cas d'absence d'exigences des propriétaires de l'information, un test sur un échantillon est mené une fois par an.

9.12 Journalisation et surveillance

L'ensemble des mesures de journalisation sont détaillées dans la procédure de journalisation [R10].

Les journaux d'évènements sont collectés et centralisés sur un serveur dédié. Les accès à ce serveur sont restreints à la DT et au RSSI.

Pour garantir la précision des journaux et leur exploitabilité, les horloges de l'ensemble du SI de Kiwi Backup sont synchronisées sur une source de référence temporelle unique.

10 Acquisition, développement et Maintenance du SI [A.14]

10.1 Sécurité dans les projets

Kiwi Backup s'assure de l'intégration de la sécurité dans les projets en imbriquant la sécurité dans sa démarche de gestion de projet.

La description des mesures de sécurité est intégrée aux documents du projet (tickets, document d'architecture technique…).

10.1.1 Analyse des risques et exigences de sécurité

Lors de la phase de spécification du projet, une analyse des risques est menée par le DT avec l'aide du RSSI. Elle permet d'établir les exigences de sécurité du projet.

Elle couvre les points suivants :

- Valeur stratégique des activités métier
- Criticité des actifs concernés
- Exigences légales, réglementaires, et les obligations contractuelles
- Exigences en disponibilité, confidentialité, intégrité et traçabilité
- Attentes des parties prenantes et les conséquences pour l'Entreprise

Les exigences de sécurité orientent l'architecture et la conception de la solution afin d'intégrer au plus tôt les mesures de sécurité nécessaires pour y répondre.

Les mesures prises par Kiwi Backup concernant l'intégration de l'analyse des risques dans les changements sont détaillées dans la politique de conception et transition des services nouveaux ou modifiés [R16] ainsi que dans la procédure de gestion des changements [R15].

10.1.2 Politique de développement sécurisé

L'ensemble des développements doivent se conformer aux bonnes pratiques de développement définies par Kiwi Backup qui s'appuient notamment sur les travaux de l'OWASP (Open Web Application Security Project) et de l'ANSSI.

Toutes les mesures prises par Kiwi Backup sont détaillées dans la politique de conception et transition des services nouveaux ou modifiés [R16].

10.1.3 Tests et audits de sécurité

Une livraison fait l'objet de tests et d'audits de sécurité conformément au programme de tests et d'audits défini lors de la phase de spécification, en accord avec les exigences de sécurité de la politique de conception et transition des services nouveaux ou modifiés [R16].

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

10.1.4 Protection des données de test

Dans la mesure du possible, Kiwi Backup utilise des données rendues anonymes ou des jeux de données créées spécialement pour effectuer ses tests, conformément à la procédure « Support et restauration de données » [R14].

Si les données utilisées dans les environnements hors production (recette, homologation, préproduction, …) sont les données de la production, ces environnements doivent bénéficier des mêmes mesures de protection que la production.

10.2 Gestion des changements

Les changements du SI de Kiwi Backup sont gérés grâce à la procédure de gestion des changements [R15]. L'organisation générale est définie dans la politique de conception et de transition de services nouveaux ou modifiés [R16].

Ce processus prévoit une appréciation du risque, une analyse des impacts du changement et une spécification des mesures de sécurité requises. L'analyse doit valider la non-compromission des mesures de sécurité existantes.

10.3 Séparations des environnements

Les environnements de développement, de test et de production doivent être séparés, conformément à la politique de conception et de transition de services nouveaux ou modifiés [R16].

11 Relations avec les fournisseurs [A.15]

11.1 Sécurité dans les relations avec les fournisseurs et sous-traitants

Toute relation avec un fournisseur ou un sous-traitant ayant accès au SI de Kiwi Backup ou à des données client est contractualisée.

Tout demandeur ou porteur d'un contrat avec un fournisseur ou un sous-traitant doit faire appel au service juridique de Kiwi Backup pour une revue du contrat avant sa signature par la direction ou par un gestionnaire habilité.

Pour tout contrat avec des sous-traitants informatiques, les contrats comprennent des clauses de sécurité en accord avec la mission confiée et les besoins de sécurité de Kiwi Backup.

La souscription aux services de fournisseurs informatiques se fait en accord avec les besoins de sécurité de Kiwi Backup.

Un accord doit être en place avant tout accès aux données de Kiwi Backup ou d'un de ses partenaires ou clients dont elle aurait la charge.

Dans le cadre des activités des services généraux, Kiwi Backup fait appel à des fournisseurs de confiance référencés et la contractualisation se fait sous-forme de devis. Ces devis ne sont pas soumis à une revue systématique du service juridique et, selon l'urgence, la contractualisation de l'intervention peut avoir lieu a posteriori.

11.2 Sécurisation de la chaine d'approvisionnement

Les exigences de sécurité sont définies lors de l'achat de produits et de services.

Les accords avec les sous-traitants et les fournisseurs encadrent leur recours à des sous-traitants :

- Sous-traitance interdite par défaut
- Pas de sous-traitance sans l'accord de Kiwi Backup, • Obligation de sécurisation de la chaîne de sous-traitance,
- Clause d'audit des sous-traitants.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Kiwi Backup se fournit en actifs informatiques directement auprès des constructeurs et des éditeurs, ou auprès de distributeurs agréés qu'elle a référencés.

Dans le cadre de ses activités de négoce et d'intégration de matériel informatique, Kiwi Backup peut être amené à mettre à jour ou modifier la configuration des logiciels embarqués (BIOS, firmware, etc …). Ces changements se font en accord avec les préconisations des fournisseurs et des éditeurs.

11.3 Surveillance et revues des services des fournisseurs et sous-traitants

Conformément aux accords conclus avec les sous-traitants et fournisseurs, Kiwi Backup s'assure par des revues ou des audits que la prestation de service assurée par le fournisseur ou sous-traitant est conforme aux attentes en matière de sécurité de l'information.

Les revues des fournisseurs ou sous-traitant peuvent se faire :
- Au travers des comités de pilotage du contrat au moins une fois par an,
- Ou à la fin d'un mandat ou d'une prestation.

Les audits des fournisseurs ou sous-traitants peuvent :
- Être effectués directement par Kiwi Backup,
- Être délégués à des tiers mandatés par elle,
- Ou s'appuyer sur des rapports émis par des tiers de confiance dans la cadre d'audit de certification ou en application de normes reconnues (ISAE 3402, ISO 27001, etc.).

Le changement et/ou l'évolution de service d'un fournisseur ou sous-traitant, doit inclure un réexamen des exigences de sécurité et des risques associés, de même si ce changement émane de Kiwi Backup, et ce, en suivant le processus de gestion des changements [R15].

L'ensemble des fournisseurs de Kiwi Backup est répertorié dans le Registre des fournisseurs-sous-traitants [R25].

12 Gestion des incidents de sécurité [A.16]

L'ensemble des collaborateurs et tierces parties doivent informer le support technique, le RSSI, le DT, de toute suspicion ou constatation d'un incident ou d'une faille de sécurité concernant le SI de Kiwi Backup.

Le support technique opère un premier tri et est en charge, si nécessaire, d'escalader l'incident et de prévenir le RSSI qui est responsable du suivi des incidents de sécurité. Les déclarations sont formalisées et tracées dans l'outil de ticketing de Kiwi Backup, Gitlab.

Tout incident de sécurité doit être géré conformément au « processus de gestion des incidents de sécurité » [R17] défini par Kiwi Backup.

13 Continuité de la sécurité [A.17]

Kiwi Backup intègre la sécurité de l'information dans son plan de continuité d'activité [R18] pour garantir la disponibilité des moyens de traitement de l'information.

Ce plan comprend :
- Le(s) scénario(s) de sinistres envisagé(s),
- Les activités critiques,
- Les acteurs essentiels ainsi que leur niveau de contribution,
- La structure de la cellule de crise et son mode d'activation,

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

- Les modalités de communication interne et externe,
- La planification des tests de continuité,
- L'amélioration du dispositif à l'issue des retours d'expérience.

Kiwi Backup met en œuvre lorsque nécessaire la redondance de ses moyens informatiques.

14 Conformité [A.18]

14.1 Conformité aux obligations légales et réglementaires

Comme précisé dans la charte d'utilisation des ressources informatiques [R2], « d'une façon générale, l'utilisation du Système d'Information doit s'effectuer dans le respect des lois, des règlements, et des usages. Chaque Utilisateur veillera à ne pas nuire aux droits et intérêts d'autrui. »

Concernant la sécurité de l'information, Kiwi Backup est soumis aux lois et réglementations suivantes :

RGPD :	Règlement européen sur la protection des données
Résumé : • Article 17 : effacer les données à caractère personnel dans les meilleurs délais sur demande de la personne concernée (droit à l'effacement ou « droit à l'oubli). • Article 20 : permettre aux utilisateurs d'exercer leur droit à la portabilité des données personnelles, soit à leur bénéfice ou celui d'un tiers. • Article 21 : permettre aux utilisateurs de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage. • Article 22 : toute personne a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. • Article 25 : disposer d'un système d'information sécurisé. • Article 33 : notifier dès que possible l'autorité nationale de protection (CNIL en France) en cas de violations graves de données afin que les utilisateurs puissent prendre des mesures appropriées. • Article 35 : consulter l'autorité de contrôle (CNIL) avant de mettre en œuvre les activités en question. • Article 37 : nommer un DPO - délégué à la protection des données. • Article 40 : l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement est encouragée.	
Décret n° 2014-1162 du 9 octobre 2014	Décret portant création d'un traitement automatisé de données à caractère personnel dénommé « Plate-forme nationale des interceptions judiciaires » (PNIJ).
Résumé : Dispositions légales permettant la mise en œuvre d'une collecte et d'un traitement automatisé de données personnelles par les autorités judiciaires, en vue de faciliter la constatation des infractions à la loi pénale.	
Code pénal	Codification du droit pénal français
Résumé : • Article 226-13 : disposition relative au secret professionnel	
Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978	Loi relative à l'informatique, aux fichiers et aux libertés

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

Résumé : • Articles 129 à 137 : traitement des données à caractère personnel	
Loi n° 2004-575 du 21 juin 2004	Loi sur la confiance en l'économie numérique (LCEN)
Résumé : Loi française sur le droit de l'Internet, sur le commerce électronique et sur la protection de la vie privée dans le secteur des communications électroniques.	
Document unique d'évaluation des risques	Obligation règlementaire liée aux conditions de travail du personnel, notamment celui ayant un impact sur la sécurité de l'information.
Résumé : L'employeur est tenu de produire une analyse des risques professionnels par tâche.	
L.1111-8 du code de la santé publique, modifié par la loi n° 2016-41 du 26 janvier 2016	Obligation règlementaire concernant l'activité d'hébergement de données de santé à caractère personnel.
Résumé : Les hébergeurs de données de santé sur support numérique (en dehors des services d'archivage électronique) doivent être certifiés. Cette certification remplace l'agrément aujourd'hui délivré par le ministère de la Santé dans les conditions définies par le décret n°2006-6 du 4 janvier 2006. Src : https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante	
Décret 2018-137 du 26 février 2018	Cadre règlementaire définissant le dépôt des demandes de certificat HDS auprès des organismes de certification.
Résumé : Définit la procédure de certification et organise la transition entre l'agrément et la certification. L'arrêté portant approbation des référentiels d'accréditation et de certification publié le 29 juin 2018 permet l'ouverture du schéma d'accréditation HDS. Les hébergeurs pourront déposer une demande de certificat HDS auprès de tout organisme de certification ayant réalisé les démarches d'accréditation auprès du COFRAC. Src : https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante	
Loi n° 94-665 du 4 août 1994 relative à l'emploi de la langue française	Obligation règlementaire définissant l'usage du français comme langue de l'enseignement, du travail, des échanges et des services publics.
Résumé : Dans la désignation, l'offre, la présentation, le mode d'emploi ou d'utilisation, la description de l'étendue et des conditions de garantie d'un bien, d'un produit ou d'un service, ainsi que dans les factures et quittances, l'emploi de la langue française est obligatoire. Src : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000349929&dateTexte=20110513	
Code de propriété intellectuelle	Cadre règlementaire définissant lesl règles en matière de droit d'auteur, propriété industrielle, artistique et littéraire.
Résumé : Définit les règles régissant les droits d'auteur et notamment celles régissant la propriété des codes source. Src : https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069414	

Les règles définies par la charte d'utilisation des ressources informatiques [R2], la présente PSSI et la documentation de sécurité permettent le respect de ces obligations.

14.2 Conformité aux obligations contractuelles

Toutes les exigences contractuelles des projets liées à la sécurité de l'information sont définies et formalisées.

Le DT s'assure que les règles de sécurité de l'information sont appliquées par ses équipes.

Selon les besoins, des engagements de confidentialité ou de non-divulgation sont signés par Kiwi Backup et ses collaborateurs.

14.3 Conformité avec la loi sur les données à caractère personnel

Kiwi Backup dispose d'un délégué à la protection des données (DPO) qui veille au respect de la législation sur les données à caractère personnel pour l'ensemble des données collectées par Kiwi Backup dans le cadre de ses activités internes.

Comme précisé dans la charte [R2], « aucun utilisateur ne pourra, sans avoir obtenu au préalable l'accord du DPO, mettre en œuvre un traitement comportant des données nominatives afin d'assurer le respect de la loi n°2018-493 du 20 juin 2018 ». »

Lorsque des données à caractère personnel sont utilisées par Kiwi Backup, elles font l'objet de mesures de protection adéquates pour garantir la conformité aux obligations légales et réglementaires en vigueur.

Dans le cas de l'utilisation de données à caractère personnel pour le compte d'un client, Kiwi Backup se conforme aux exigences définies par le client dans le contrat de service.

14.4 Evaluation de la conformité ou revue de la SSI

Kiwi Backup procède à des revues régulières de sa sécurité grâce au comité de sécurité (COSEC), aux revues
de Direction, aux remontées d'indicateurs, et des audits internes portant à la fois sur les parties organisationnelles et techniques de la sécurité de l'information.

Les revues de Direction et les remontées d'indicateurs donnent lieu à des plans d'actions suivis par le comité de sécurité.

Les audits donnent lieu à des rapports et plans d'actions qui sont présentés au comité de sécurité et à la Direction.

14.5 Gestion des dérogations

Toute dérogation aux règles définies par la charte d'utilisation des ressources informatiques [R2], la présente PSSI et la documentation de sécurité doit donner lieu à une demande écrite pour validation auprès du RSSI au travers de l'outil de ticketing de Kiwi Backup.

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

ANNEXE 4 – LETTRE D'ENGAGEMENT DE LA DIRECTION de KIWI BACKUP
https://www.kiwi-backup.com/actualite/kiwi-backup-lettre-engagement-direction-certification-hds/

Depuis plus de 15 ans, Kiwi Backup vous accompagne dans la sauvegarde de vos données sensibles et, depuis 2018, de vos données de santé.
Conformément à l'évolution de la réglementation concernant l'hébergement et l'infogérance des données de santé, Kiwi Backup s'est engagé dans un processus de certification HDS comprenant le respect de la **norme ISO 27001**.
Lettre d'engagement de la Direction
Afin d'accompagner les exigences de sécurité de plus en plus fortes de nos clients et d'assurer la pérennité de la solution Kiwi Santé, Kiwi Backup s'est engagé dans un processus de certification HDS, comprenant notamment le respect de la norme ISO 27001, une norme liée au management de la sécurité des systèmes d'information.
Cette démarche s'inscrit pleinement dans nos valeurs de confiance, de professionnalisme, d'innovation et de dynamisme. Dans cette perspective, notre principal objectif est d'assurer un développement durable de Kiwi Backup, tout en mettant en œuvre des conditions maximales de sécurité pour les processus et les données et en assurant la qualité de la solution.
La certification HDS est particulièrement exigeante, et ce d'autant plus pour des ESN de petite taille comme Kiwi Backup. Néanmoins, elle est indispensable sur un marché comme le nôtre, nos clients nous confiant leurs biens parmi les plus précieux : leurs données sensibles et données de santé. Nous nous engageons à répondre à leur légitime demande de sécurisation via cette démarche de certification.
Ainsi, un système de management de la sécurité des informations (SMSI) a été mis en place durant le premier semestre 2019. Celui-ci comprend des politiques de haut niveau établissant les exigences de Kiwi Backup envers l'ensemble de ses processus et de ses relations avec son environnement (clients, fournisseurs, salariés, législateur, …), mais également des procédures détaillées pour chaque action faisant intervenir la sécurité. Un système de management des services (SMS) a également été initié afin de mettre la sécurité des données et la continuité des services au cœur des développements réalisés.
Pour soutenir et alimenter cette démarche, une analyse de risques a été mise en œuvre en s'appuyant sur la méthodologie EBIOS de l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Cette analyse permet d'identifier les menaces les plus critiques et de mettre en place les actions nécessaires, revues régulièrement en comité de sécurité.
Les hommes et femmes composant Kiwi Backup étant sa plus grande richesse, de par leurs compétences et leurs savoir-faire, tous sont engagés dans ce processus et sont acteurs de la sécurité au quotidien à tous les niveaux. Un processus de sensibilisation continue des salariés aux enjeux de la sécurité et des formations régulières pour certains personnels-clés, notamment administrateurs systèmes et RSSI, ont été mis en place. L'implication de tous est primordiale et je remercie l'ensemble du personnel pour leur adhésion depuis le début du projet et leurs contributions à venir.
La certification HDS en elle-même est une étape clé, mais ne représente qu'un jalon dans le processus mis en œuvre dans la société. Des audits annuels nous permettrons de nous assurer que la démarche d'amélioration continue et le suivi de nos plans d'action au quotidien répondent bien aux enjeux en présence : sécurisation des processus et des données, réponses aux exigences de nos clients en matière de sécurité et respect des réglementations en vigueur dans notre secteur d'activité.
Je m'engage personnellement à ce que l'ensemble des dispositions prises dans le SMSI et le SMS de Kiwi Backup soient appliquées et respectées et à fournir les moyens nécessaires pour cela aux équipes Kiwi Backup.
Mulhouse, le 10 septembre 2019
Sébastien HEITZMANN
Gérant et Directeur Technique Kiwi Backup

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

ANNEXE 5 – CERTIFICAT HDS OVH

Certificat
Certificate

LABORATOIRE NATIONAL DE MÉTROLOGIE ET D'ESSAIS

Numéro de certificat 36048-0
Certificate number

OVH

2 Rue Kellermann 59100 - ROUBAIX - FRANCE

met en œuvre et entretient un système de management conforme au référentiel de certification,
operates a management system which complies with the requirements of,

Hébergeur de Données de Santé version 1.1 juin 2018 - ASIP SANTE

Pour les activités suivantes / for the following activities

offre commerciale "OVH Healthcare Serveurs Dédiés" concernant :
commercial offer "OVH Healthcare Dedicated servers" regarding :

Hébergeur d'infrastructure physique	Physical infrastructure hosting provider
1. La mise à disposition et la maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé	1. Provision and maintenance service of physical sites hosting information system material infrastructure used to process health data
2. La mise à disposition et la maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé	2. Provision and maintenance service of information system material infrastructure used to process health data
Hébergeur Infogérant	Service hosting provider
3. La mise à disposition et la maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information	3. Provision and maintenance service of information system application hosting platform
4. La mise à disposition et la maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé	4. Provision and maintenance service of information system virtual infrastructure used to process health data
5. La sauvegarde de données de santé	5. Back up of health data

Déclaration d'applicabilité / Statement of applicability
SoA–Dedicated_Servers version 28 du 15 juillet 2019 et SOA_Datacenter version 8.7 du 29 mai 2019

Ce certificat est valide sous réserve de la validité du certificat référencé :
This certificate is valid subject to the validity of certificate referenced :
ISO 27001 : 2013

Site(s) concerné(s) / Concerned location(s)
voir annexe / see annex

Date début de validité 10 octobre 2019
Effective date October 10th, 2019

Valable jusqu'au 09 octobre 2022
Expiry date October 9th, 2022

Pour le Directeur Général
For the General Director

Laboratoire national de métrologie et d'essais

Responsable du Pôle Certification Instrumentation et Technologies de l'Information
Head of the Instrumentation and IT Certification Department

cofrac
CERTIFICATION DE SYSTÈMES DE MANAGEMENT
Accréditation n°4-0056
Liste des sites accrédités et portée disponible sur www.cofrac.fr

HDS-V1-062019

Ce certificat est délivré conformément aux règles générales de certification LNE des systèmes de management d'entreprise.
This certificate is granted under the LNE regulations for registration.

Laboratoire national de métrologie et d'essais - 1, rue Gaston Boissier – 75724 PARIS Cedex 15

ANNEXE 6 – CERTIFICAT ISO 27001 de l'EDITEUR

CERTI TRUST
CONFIDENCE IN THE DIGITAL ERA

CERTIFICAT

ICTS certifie par la présente que le système de management de

KIWI BACKUP

40, rue Victor Schoelcher
68100 Mulhouse
France

A été évalué en accord avec les exigences de système de management reprises dans

ISO/CEI 27001:2013

Déclaration du champ d'application de la certification :

Le système de management de la sécurité de l'information (SMSI) de Kiwi Backup Le SMSI couvre l'ensemble des processus de gestion ainsi que des processus de support de la solution de sauvegarde de données pour les professionnels de la santé commercialisée sous le nom de Kiwi Santé. Ceci est conforme avec la Déclaration d'Applicabilité (version 2.3 du 19 septembre 2019).

Certificat N° **C-ISMS-112019-0CU00263**

Certification initiale : **20-11-2019**
Début du cycle actuel de certification : **20-11-2019**
Certificat valide du **20-11-2019** au **19-11-2022**
**Sujet à des audits de surveillance annuels*

Luxembourg, **20-11-2019**

Pierre Dewez,
Directeur Général.

INTERDIGICERT EUROPE SA
a CERTI-TRUST™ brand
36, Dernier Sol
L-2543 Luxembourg
G.-D. de Luxembourg
+352 (0)20 30 10 43
+352 (0)27 00 08 33
info.services@certi-trust.com

ISO 27001 CERTI TRUST

ACCREDITATION ISO/IEC 17021-1
MLA-MRA Signatory

Cette évaluation et la certification associée ont été menées dans le respect des procédures d'audit et de certification d'Interdigicert Europe. Ce certificat peut être vérifié en envoyant un e-mail à certification@certi-trust.com.

Page 1 de 2

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan

ANNEXE 7 – CERTIFICAT HDS de l'EDITEUR

CERTI TRUST
CONFIDENCE IN THE DIGITAL ERA

CERTIFICAT

ICTS certifie par la présente que

KIWI BACKUP

40, rue Victor Schoelcher
68100 Mulhouse
France

A été évaluée en accord avec les exigences reprises dans le

Référentiel HDS:2018

(Hébergeur de Données de Santé – version 1.1)

en tant que

Hébergeur Infogéreur

Déclaration du champ d'application de la certification :

Le périmètre retenu pour l'hébergement de données de santé adresse la mise à disposition et le maintien en condition opérationnelle : de la plateforme d'hébergement d'applications du système d'information (activité 3) ; de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé(activité 4) ; ainsi que l'administration et l'exploitation du système d'information contenant les données de santé (activité 5) et leur sauvegarde (activité 6).

Certificat N° **C-HDS-012020-0CU00263**

Paris, **31-01-2020**

basé sur le(s) certificat(s) suivants :

☑ *France : ISO/CEI 27001:2013 n° C-ISMS-112019-0CU00263 (Certi-Trust)*

Certification initiale : **31-01-2020**
Début du cycle actuel de certification : **31-01-2020**
Certificat valide du **31-01-2020** au **30-01-2023**
**Sujet à des audits de surveillance annuels.*

Pierre Dewez,
Directeur Général.

ICTS FRANCE sàrl
Groupe CERTI-TRUST™
27, Place de la Madeleine
F-75008 Paris
France
: +33 (0)1 86 86 22 08
: info.services@certi-trust.com

HDS CERTI TRUST

cofrac
CERTIFICATION DE SYSTEMES DE MANAGEMENT
Certification de systèmes de management
NF EN ISO/IEC 17021-1:2015
Accréditation n°4-0612 rev.0
Liste des portées disponibles sur www.cofrac.fr

Cette évaluation et la certification associée ont été menées dans le respect des procédures d'audit et de certification d'ICTS. Ce certificat peut être vérifié en envoyant un e-mail à certification@certi-trust.com.

Page 1 de 2

Alp2i Medical Solutions by Trilog - Sarl au capital de 7622 € - RCS de Grenoble : 419 283 528
Siège social : 11, chemin du Vieux Chêne 38240 Meylan