GROUPE EVOLUCARE

CONDITIONS SPECIFIQUES HEBERGEMENT

V2020.12.03

1- DEFINITIONS

Pour les besoins des présentes Conditions Spécifiques et nonobstant toute autre définition prévue dans les Conditions Communes, les présents termes commençant par une majuscule, qu'ils soient au singulier ou au pluriel, ont la signification suivante :

Anomalie : tout dysfonctionnement, erreur, panne répétitif et reproductible trouvant son origine dans l'exécution du Service Hébergement, imputable à la Société et affectant de façon substantielle l'utilisation ou le fonctionnement du Service Hébergement.

Autorisations Nécessaires : les autorisations et/ou licences devant être obtenues par le Client auprès de tiers aux fins de permettre à la Société, ainsi qu'aux sous-traitants de la Société, en particulier à l'Hébergeur Certifié HDS, d'utiliser et d'exploiter les différents éléments mis à disposition de la Société par le Client dans le cadre du Contrat, tels que les Progiciels Tiers. La Société se réserve le droit de demander à tout moment communication de ces autorisations et licences au Client.

Data Center : le ou les centres d'hébergement physique (locaux) de la Plateforme d'Hébergement, dont l'adresse – à la Date d'Entrée en Vigueur – et les conditions de sécurité sont définies en annexe 2 ; le choix du Data Center étant à la discrétion de la Société, sous réserve que celui-ci soit localisé en France. Toute modification de la localisation du Data Center faisant l'objet d'une information écrite par la Société au Client.

Données : toutes données et informations saisies, générées, produites, stockées ou traitées par le Client et/ou les Utilisateurs, par le biais du Progiciel en Mode Hébergé et hébergées dans le cadre du Service Hébergement. Les Données sont et demeurent la propriété du Client dans les limites définies par la loi.

Données de Connexion : l'identifiant et le mot de passe correspondant à chaque Utilisateur et permettant l'accès au Progiciel en Mode Hébergé.

Données Biométriques : les Données à Caractère Personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

Durée : la durée initiale du Service Hébergement telle que définie au Bon de Commande, et toute extension selon les modalités prévues aux Conditions Communes s'agissant des Services Récurrents, sauf résiliation anticipée.

Environnement Client : l'équipement informatique installé chez le Client (matériels, système d'exploitation, bases de données, logiciels, souscription à un service

d'accès internet) et connecté à la Plateforme d'Hébergement pour les besoins de la réalisation du Service Hébergement, appartenant au Client et/ou dont le Client détient la jouissance des droits nécessaires à la conclusion et à l'exécution du Contrat. L'Environnement Client doit être conforme aux Prérequis Techniques, tels que définis au Bon de Commande correspondant.

Hébergement de Données de Santé : les prestations d'hébergement de Données de Santé sur la Plateforme d'Hébergement conformes à l'article L.1111-8 du Code de la santé publique issu de l'Ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel et à son décret d'application n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel.

Hébergeur de Données de Santé ou Hébergeur Certifié HDS : la personne morale fournissant les services d'Hébergement de Données de Santé, certifiée HDS.

Infrastructure : les équipements informatiques (infrastructure télécom, matériels et logiciels) sur lesquels le Progiciel est hébergé.

Niveaux de Service (« SLA ») : sous réserve des stipulations spécifiques à l'Hébergement de Données de Santé en annexe 3, les engagements de la Société, relatifs au Service Hébergement, tels que décrits en annexe 1 des Conditions Spécifiques.

Phases : les étapes du déroulement de l'exécution du Service Hébergement telles que décrites à l'article 3.1 et en annexe 1, comprenant :

- **la « Phase Préparatoire » :** la période comprise entre la Date d'Entrée en Vigueur et la mise en production de la Plateforme d'Hébergement, au cours de laquelle la Société fournit au Client certaines Prestations (notamment, démarrage, paramétrages, tests…) permettant ladite mise en production de la Plateforme d'Hébergement.
- la **« Phase de Service Régulier » :** la phase d'exploitation du Progiciel en Mode Hébergé, dans un contexte « production ». Le Service Hébergement en Phase de Service Régulier est un Service Récurrent.

et, le cas échéant,

- la **« Phase de Réversibilité »** : la phase optionnelle décrite à l'article 8, consistant à la fourniture de Prestations additionnelles d'assistance du Client dans le cadre de la reprise du Service Hébergement directement par le Client, ou par un prestataire désigné par le Client.

Plateforme d'Hébergement : l'infrastructure technique (logiciels, matériels) appartenant à la Société ou que la Société est autorisée à utiliser pour les besoins de son activité, connectée à des réseaux de télécommunications la reliant à Internet, abritant le Progiciel en Mode Hébergé et les Données, et mise à disposition du Client, pour les stricts besoins de l'exécution du Contrat. La Plateforme d'Hébergement - dans sa version à la Date d'Entrée en Vigueur – est décrite en annexe 2.

Prestations : les prestations de services associées non-récurrentes - notamment les prestations de conseil, de formation et/ou d'assistance dans le cadre de la Phase Préparatoire et/ou dans le cadre de la Phase de Réversibilité - pouvant être fournies par la Société au Client soumises aux Conditions Spécifiques applicables, telles que définies dans la rubrique distincte du Bon de Commande ou un Bon de Commande séparé le cas échéant.

Progiciel : le Progiciel en Mode Acquisition ou en Mode SaaS, objet de la Licence correspondante, ainsi que, le cas échéant, les Mises à Jour mises à disposition du Client dans le cadre des Services Maintenance et d'Assistance, au titre du (des) Bon(s) de Commande correspondant(s).

Progiciel en Mode Hébergé : le Progiciel et/ou le Progiciel Tiers hébergé(s) sur la Plateforme d'Hébergement selon les termes du Contrat.

Profil Utilisateur : le profil de l'Utilisateur qui détermine les fonctionnalités du Progiciel et le cas échéant du Progiciel Tiers, qui lui sont accessibles.

Progiciel Tiers : la ou les applications non éditées par la Société, appartenant au Client et/ ou dont le Client détient la jouissance des droits nécessaires à la conclusion et à l'exécution du Contrat, hébergées sur la Plateforme selons les termes du Contrat.

Service Hébergement / Hébergement : le service par lequel la Société met à disposition du Client le Progiciel en Mode Hébergé, afin de rendre accessibles au Client, le Progiciel ou le Progiciel Tiers, et les Données selon les termes du Contrat. L'Hébergement comprend la maintenance de la Plateforme d'Hébergement.

Utilisateur(s) : selon le Progiciel ou Progiciel Tiers concerné, le Client, lui-même, personne physique, professionnel de santé inscrit auprès des instances compétentes, ou toute personne physique sous la responsabilité du Client (notamment professionnel de santé sous contrat avec le Client, salarié, préposé, prestataire, représentant),

identifiée et autorisée par le Client – en fonction de son Profil Utilisateur - , à utiliser le Progiciel en Mode Hébergé sur son terminal informatique dans le strict respect du Contrat et de la Documentation.

Les autres termes utilisés aux présentes commençant par une majuscule et non définis aux présentes, auront entre les Parties, la signification qui leur est donnée dans les Conditions Communes.

2- OBJET

Les présentes Conditions Spécifiques régissent les termes et conditions selon lesquels la Société fournit au Client le Service Hébergement. Elles complètent les Conditions Communes ; étant rappelé que le Progiciel objet du Bon de Commande correspondant est soumis aux Conditions Spécifiques applicables à la Licence en Mode Acquisition ou en Mode SaaS, et que les Services Maintenance et Assistance y afférents sont soumis aux Conditions Spécifiques applicables auxdits Services Maintenance et Assistance.

Il est rappelé qu'en cas de contradiction entre les Conditions Communes et les Conditions Spécifiques, les Conditions Spécifiques prévalent.

Le Service Hébergement étant susceptible de constituer, compte-tenu de la nature des Données traitées par le Progiciel en Mode Hébergé, un Hébergement de Données de Santé, les présentes Conditions Spécifiques comprennent un certain nombre de stipulations spécifiques applicables à ce type d'hébergement et de données, conformément à la réglementation applicable en la matière, et qui figurent en annexe 3 des Conditions Spécifiques. Il est précisé que s'agissant de l'Hébergement de Données de Santé, les stipulations de l'annexe 3 prévalent sur toute autre stipulation des présentes Conditions Spécifiques.

Dans ce contexte, la Société a recours à un Hébergeur de Données de Santé Certifié HDS, à qui elle sous-traite l'Hébergement de Données de Santé ; la Société n'étant pas Hébergeur de Données de Santé.

Les Parties conviennent que, sur les aspects liés à l'Hébergement de Données de Santé, le Contrat pourra devoir être complété afin d'en assurer la complétude et la conformité aux éventuelles modifications de la réglementation qui pourraient intervenir en cours d'exécution.

3- SERVICE HEBERGEMENT

Le Service Hébergement à la Date d'Entrée en Vigueur, est décrit de façon exhaustive en annexe 1 ; le Périmètre étant défini dans le Bon de Commande.

La Société choisit librement l'hébergeur, en particulier l'Hébergeur de Données de Santé Certifié HDS, qui est son sous-traitant. La Société reste seule responsable vis-à-vis du Client du respect des engagements pris aux présentes.

La Société assure l'Hébergement du Progiciel sur la Plateforme d'Hébergement dans le(s) Data Center(s), et ce conformément aux termes définis en annexes des Conditions Spécifiques ; étant précisé que la Société conserve la gestion des liens réseaux internes au(x) Data Center(s).

Le Client reconnaît et accepte que la Société peut :

- transférer la Plateforme d'Hébergement d'un Data Center à un autre et à sa seule discrétion et à ses frais, sous réserve d'en informer le Client par quelque moyen que ce soit, que le nouveau Data Center soit localisé dans l'Espace Economique Européen, et présente un niveau de sécurité conforme à ses engagements contractuels et à l'état de l'art.
  Les Parties échangeront et définiront ensemble en temps utile, les modalités et la durée d'interruption nécessaires au transfert de la Plateforme d'Hébergement vers le nouveau Data Center ;
- modifier à sa convenance les moyens et ressources mis en œuvre pour réaliser l'Hébergement, étant entendu que la Société s'engage, tout au long de la Durée, à maintenir la Plateforme d'Hébergement à un niveau de dimensionnement compatible avec les Niveaux de Service et le Progiciel en Mode Hébergé, sous réserve que le Progiciel en Mode Hébergé soit utilisé conformément à sa destination et à sa Documentation.

3.1 Calendrier d'exécution ; Phase Préparatoire et Phase de Service Régulier

L'Hébergement se déroulera en deux (2) Phases : une Phase Préparatoire et une Phase de Service Régulier, dont les modalités sont décrites en annexe 1.

Pour la bonne exécution du Service Hébergement, les Parties ont établi un calendrier d'exécution définissant :

- les dates de début et de fin pour chaque Phase (à l'exception de la Phase de Réversibilité, qui par nature, ne peut être prévue à la Date d'Entrée en Vigueur du Contrat) ;
- les prérequis d'entrée dans chaque Phase ;
- les livrables associés à chaque Phase.

Le calendrier d'exécution est défini au Bon de Commande.

Le Client reconnaît et accepte que le respect du calendrier d'exécution par la Société dépend en partie de sa propre collaboration active et régulière.

Les modalités de recette de mise à disposition du Service Hébergement sont décrites en annexe 1. Il est toutefois d'ores et déjà entendu que la recette par le Client des Prestations effectuées dans le cadre de la Phase Préparatoire par la Société vaudra recette du Service Hébergement. De plus, toute utilisation du Service Hébergement par le Client, et en particulier toute connexion au Progiciel en Mode Hébergé par un ou plusieurs Utilisateurs, vaudra recette du Service Hébergement.

Afin de lever toute ambiguïté, il est précisé que la Société n'est pas encore tenue par les engagements de Niveaux de Service pendant la Phase Préparatoire, et ce en raison de la nature même de ladite Phase.

3.2 Modalités d'exécution du Service Hébergement

3.2.1 Prérequis

Le Client reconnaît que, s'agissant de l'Hébergement du Progiciel, le maintien en vigueur de la Licence constitue un prérequis à la conclusion et au maintien en vigueur du Service Hébergement, et que la mise à disposition des Mises à Jour du Progiciel implique la souscription et le maintien en vigueur des Services Maintenance et Assistance.

S'agissant de l'Hébergement du Progiciel Tiers, le Client garantit qu'il détient et qu'il détiendra les Autorisations Nécessaires au fonctionnement et à l'Hébergement du Progiciel Tiers et à l'exécution du Contrat, et ce pendant toute la Durée. Si la Société avait à utiliser, exploiter, et/ou modifier au cours de l'exécution du Contrat des éléments non prévus à la signature du Contrat, le Client obtiendrait les Autorisations Nécessaires requises aussi préalablement à leur remise à la Société pour permettre leur utilisation, leur exploitation et/ou leur modification par ce dernier dans le respect des droits des tiers.

Le Client reconnaît que toute modification de l'Environnement du Client ayant des impacts sur l'Hébergement, ainsi que toute modification du Progiciel Tiers ou de ses préconisations techniques, est susceptible d'avoir des impacts sur la fourniture du Service Hébergement par la Société ainsi que sur les conditions financières qui devraient être revues en conséquence. Afin de lever toute ambiguïté, il est précisé que le Client n'est autorisé à accéder à la Plateforme d'Hébergement qu'aux fins exclusives d'accéder et d'utiliser le Progiciel en Mode Hébergé.

La Société ne supporte aucune responsabilité sur le contenu et l'utilisation du Progiciel Tiers hébergé sur la Plateforme d'Hébergement, lequel sont sous l'entière responsabilité du Client.

Le Client reconnaît et accepte que la définition précise, exhaustive et stable de ses besoins est essentielle à la bonne réalisation du Service Hébergement. Tout surcoût consécutif à une mauvaise évaluation de

ses besoins ou à un défaut d'information de la part du Client sur lesdits besoins, est à la charge du Client.

En outre, le Client est seul responsable :

- en ce qui concerne l'Hébergement de Progiciel Tiers, de la mise en œuvre et de la gestion à ses frais – directement ou indirectement par l'intermédiaire d'un tiers – du Progiciel Tiers ;
- de manière générale :
    - de la mise en œuvre et de la gestion à ses frais - directement ou indirectement par l'intermédiaire d'un tiers - de l'ensemble de l'Environnement Client et services nécessaires ou utiles pour accéder au Progiciel en Mode Hébergé et ce, en conformité avec les Prérequis Techniques ; le Client devant s'assurer de la compatibilité de ses systèmes et de l'Environnement Client avec la Plateforme d'Hébergement et que le format des Données est supporté par les systèmes de la Plateforme d'Hébergement ;
    - du bon fonctionnement des éléments qui précèdent, et en particulier des liens de télécommunications nécessaires pour accéder au Progiciel en Mode Hébergé, qui constituent un Prérequis Technique à l'exécution du Service Hébergement par la Société ; étant précisé que la Société recommande fortement la mise en place d'une ligne dédiée et ce, dans un souci de sécurité. Si le Client ne retient pas la proposition de la Société, et donc ne confie pas de façon expresse à la Société la mise en place d'une telle ligne, la Société n'est en aucun cas responsable des problèmes ou dommages relatifs à des lignes louées à un prestataire extérieur. La Société ne peut être tenue responsable du fait d'un dysfonctionnement du Service Hébergement de quelque nature que ce soit, en ce compris toute violation de sécurité ou perte de performance, qui résulterait du défaut de mise en place d'une ligne dédiée dans les conditions susvisées.

3.2.2 Accès au Progiciel en Mode Hébergé

L'accès au Progiciel en Mode Hébergé nécessite l'utilisation de Données de Connexion.

Les Données de Connexion sont destinées à réserver l'accès au Progiciel en Mode Hébergé aux Utilisateurs, à protéger l'intégrité et la disponibilité du Progiciel en Mode Hébergé ainsi que l'intégrité, la disponibilité et la confidentialité des Données.

La Société fournira au Client l'accès au Progiciel en Mode Hébergé pour au moins un (1) Utilisateur (l'administrateur désigné par le Client, tel que défini au Bon de Commande). A compter de la date de cette fourniture, le Service Hébergement sera réputé accessible par le Client.

L'accès au Progiciel en Mode Hébergé est effectué à partir de l'Environnement Client, au moyen des Données de Connexion attribuées aux Utilisateurs par l'Utilisateur désigné comme administrateur par le Client. Chaque Utilisateur est tenu de les utiliser lors de chaque connexion.

Le Client est seul responsable de la gestion des habilitations et de l'attribution des Données de Connexion à ses Utilisateurs, et tout Utilisateur est le titulaire de ses Données de Connexion. De manière générale, le Client reste seul responsable de l'utilisation du Progiciel en Mode Hébergé par les Utilisateurs.

Les Données de Connexion sont personnelles et confidentielles. En conséquence, il appartient aux Utilisateurs et à l'interlocuteur privilégié de mettre en œuvre toutes mesures de précaution et de sécurité, pour conserver celles-ci confidentielles et pour que celles-ci ne soient pas divulguées à des tiers. Tout accès au Progiciel en Mode Hébergé par le biais de ces Données de Connexion sera réputé fait pour le compte du Client sous la responsabilité du Client. Dans ce cadre, et en raison du caractère informatique des Prestations, le Client accepte expressément que l'ensemble des données sous forme électronique, quel que soit leur support, notamment les logs de connexion, fichiers informatiques, identifiants, informations d'horodatage, messages, emails et autres, émanant du système informatique de la Société et de ses sous-traitants, lui soient pleinement opposables.

Le Client s'engage à ne pas contester la recevabilité, la validité et l'opposabilité de tels éléments de preuve au motif de leur nature dématérialisée et reconnaît que ces éléments feront foi de la réalité des opérations.

Le Client est seul responsable de l'utilisation et de la conservation des Données de Connexion. Si le Client accorde à l'un de ses prestataires, par exemple l'éditeur du Progiciel Tiers, un droit d'accès à la Plateforme d'Hébergement et/ou au Progiciel Tiers, le Client est intégralement responsable de cet accès et des conséquences qui pourraient en résulter.

Toutes conséquences préjudiciables résultant de la divulgation ou d'un accès non autorisé aux Données de Connexion devront être intégralement réparées par le Client.

La Société ne pourra être responsable de toutes conséquences liées à une divulgation ou à un accès non autorisé, délibéré ou non, aux Données de Connexion.

Dans l'hypothèse où le Client soupçonnerait ou aurait connaissance d'une perte ou vol des Données de Connexion ou d'un accès ou d'une divulgation frauduleuse ou non autorisé(e) des Données de Connexion il s'engage à procéder immédiatement (i) au changement des Données de Connexion selon la procédure mise en place par la Société et (ii) à en informer la Société par écrit.

3.3 Continuité et disponibilité de l'accès au Progiciel en Mode Hébergé

La Société s'engage à mettre en œuvre les moyens appropriés au regard de l'état de la technique et dont elle a connaissance, en vue de fournir le Service Hébergement de manière continue, selon les termes du Contrat, et en particulier selon les Niveaux de Service définis en annexe 1 pendant la Phase de Service Régulier.

De convention expresse, la Société peut restreindre ou suspendre la fourniture du Service Hébergement - sans indemnité et sans préjudice des sommes dues au titre du Contrat, en cas de maintenance programmée tel que prévu en annexe 1.

Toute interruption planifiée devra être effectuée en respectant les conditions figurant dans l'annexe 1, étant entendu que la Société s'efforcera de respecter un préavis raisonnable, sauf dans les cas d'urgence. La durée de l'interruption dépendra du type d'intervention à réaliser.

3.4 Sécurité

3.4.1 Chacune des Parties s'engage à mettre en œuvre les moyens appropriés au regard de l'état de la technique et dont elle a connaissance, afin d'empêcher (i) tout accès frauduleux à la Plateforme d'Hébergement et au Progiciel en Mode Hébergé, et (ii) que les Données ne soient détruites, perdues, indisponibles, altérées ou divulguées à toute personne non autorisée à les connaître.

En particulier, la Société s'engage à mettre en œuvre les moyens organisationnels et techniques et les mesures administratives appropriés, et à prendre les précautions utiles, conformes à l'état de l'art en particulier pour le traitement des Données de Santé et Données Biométriques le cas échéant, en vue de préserver la sécurité, l'intégrité et la confidentialité des Données dans le cadre de l'exécution du Contrat.

A cet effet et sous réserve de toutes stipulations spécifiques du Contrat relatives aux Données de Santé :

- la Société met en place les procédures de sécurité et de sauvegarde conformément aux Niveaux de Service tels que décrits en annexe 1 ;
- plus généralement, les conditions dans lesquelles la sécurité du Data Center est assurée sont décrites dans l'annexe 2 « Plan Assurance Sécurité » ;

Nonobstant ce qui précède, le Client reconnaît être informé qu'en l'état de la technique, la Société ne peut garantir l'absence d'intrusion dans la Plateforme d'Hébergement d'une part, ni l'absence de modification, destruction ou d'altération des Données, notamment du fait d'un Code Malveillant et ce, y compris par un Utilisateur, d'autre part.

3.4.2 En outre, la Société se réserve la possibilité d'exercer des contrôles sur la conformité de l'utilisation par le Client du Progiciel et de la Plateforme d'Hébergement ; la Société peut prendre toute mesure utile ou suspendre temporairement l'accès du Client au Service Hébergement, en cas d'utilisation illégale, de piratage ou de contrefaçon du Progiciel, ou en cas de risque particulier pour la sécurité de l'Hébergement du Progiciel et des Données, ou si la Société estime raisonnablement que le Service Hébergement ou tout composant de celui-ci sont susceptibles de subir une menace importante pour la sécurité, ou que son contenu apparaît comme manifestement illicite et/ou dans le cas où la Société a connaissance d'un risque pour son utilisation, son bon fonctionnement, la sécurité, non-conformité aux prescriptions légales et réglementaires applicables. Dans la mesure du possible, la Société informe le Client de cette suspension à l'avance, sauf dans les cas d'urgence. En aucun cas, une telle suspension du Service Hébergement ne peut être considérée comme un manquement par la Société à ses obligations contractuelles, ni être prise en compte dans le calcul du temps de disponibilité prévue en annexe 1 et/ou en tout état de cause, ne peut donner lieu à une quelconque indemnité au profit du Client, sans préjudice des autres droits et dommages et intérêts auxquels la Société pourrait prétendre.

Cette suspension ne libère pas le Client de ses obligations de paiement des sommes dues au titre du Contrat.

3.5 Données

3.5.1 Le Client (ou, le cas échéant, les Utilisateurs) reste(nt) seul(s) propriétaire(s) des droits associés aux Données.

Le Client accorde à la Société, pour la Durée, un droit d'accès et d'utilisation des Données dans le but d'exécuter les Services Hébergement et/ou d'exécuter ses obligations en vertu du Contrat.

Les Données sont réputées être des Informations Confidentielles.

Le Client garantit qu'il dispose de toutes les autorisations d'utilisation et/ou de diffusion des informations et Données de toute nature, hébergées par la Société au titre du Contrat, y compris les Données à Caractère Personnel.

Le Client s'engage à fournir des Données loyales et de qualité, conformes à la législation et aux réglementations en vigueur, et aux usages, notamment et de manière non limitative, ceux qui régissent le fonctionnement des services en ligne, le commerce, la protection des mineurs, le respect de la personne humaine et la propriété intellectuelle sous sa seule responsabilité.

En conséquence, la Société ne pourra être tenue responsable en cas de non-conformité ou contravention des Données aux lois et règlements, à l'ordre public, aux droits des tiers (de quelque nature que ce soit).

En outre, le Client reconnaît que certaines Données hébergées sont couvertes par le secret médical et que le Client est garant du respect du secret médical par les Utilisateurs et de manière générale, son personnel et le cas échéant de ses sous-traitants.

Le Client est seul responsable de la nature et de la qualité des Données et de leur transmission, intégration et traitement dans le cadre de l'Hébergement, y compris des conséquences de leur mise à disposition du public, fût-il restreint sur Internet. En aucun cas, la Société ne peut être tenue responsable du contenu et du contrôle des Données.

La Société s'engage à assurer la confidentialité et la sécurité des Données conformément aux termes de l'annexe 1.

La Société ne supporte aucune responsabilité sur le contenu des Données hébergées sur la Plateforme d'Hébergement, lesquelles sont sous l'entière responsabilité du Client.

3.5.2 Ainsi, le Client garantit que les Données ne donneront pas lieu à des réclamations de tiers, y compris des réclamations relatives aux Droits de Propriété Intellectuelle de tiers, à du matériel pornographique, à de la diffamation, à des violations de la vie privée, ou à d'autres droits de tiers.

Dans ce cadre, le Client s'engage à défendre et indemniser la Société contre toute action en justice ou réclamation alléguant que les Données portent atteinte aux droits de tiers, y compris les Droits de Propriété Intellectuelle. Le Client indemnisera la Société du montant de toute condamnation ou indemnité transactionnelle et de tout frais en lien avec cette réclamation, en particulier les frais d'avocats.

3.6 Stipulations spécifiques applicables aux Données de Santé

Le traitement de Données de Santé implique le respect par chaque Partie des dispositions légales et réglementaires applicable à ce secteur, en particulier, dans le cadre des présentes Conditions Spécifiques, celles relatives à l'Hébergement des Données de Santé.

Conformément à la réglementation applicable et en particulier aux dispositions du Code de la santé publique, les Données de Santé seront hébergées auprès d'un l'Hébergeur Certifié HDS.

Cet Hébergeur Certifié HDS est, au jour de la signature des présentes, précisé en annexe 3. La Société se réserve toutefois le droit de changer d'Hébergeur Certifié HDS à tout moment de l'exécution du Contrat, sous réserve d'en informer le Client avec un préavis suffisant.

L'annexe 3 « Spécificités liées à l'Hébergement de Données de Santé » décrit les droits et obligations respectifs des Parties liées à la nature spécifique des Données de Santé hébergées.

La Société se réserve le droit de compléter et/ou amender cette annexe, même après signature des présentes, en particulier afin d'assurer la conformité du Contrat avec (i) ses obligations légales et réglementaires en matière d'Hébergement de Données de Santé ainsi qu'avec (ii) le contenu du contrat entre la Société et l'Hébergeur Certifié HDS.

4. DONNEES A CARACTERE PERSONNEL

4.1 Au sens du RGPD, et dans le cadre du Service Hébergement, le Client est responsable du traitement, et la Société est sous-traitant.

Dans ce cadre, la Société est autorisée pendant toute la Durée à traiter pour le compte du Client les Données à Caractère Personnel, et ce incluant des Données de Santé et/ou des Données Biométriques strictement nécessaires à l'exécution du Service Hébergement.

4.2 La Société, en sa qualité de sous-traitant, s'engage pour sa part, à traiter les Données à Caractère Personnel dans le cadre strict et nécessaire à l'exécution du Contrat et à n'agir que sur les seules instructions documentées du Client.

4.3 Dans le cadre du Service Hébergement l'hébergeur sous-traitant choisi par la Société, Certifié HDS, agit en qualité de « sous-traitant ultérieur » au sens des Lois et Réglementations sur la Protection des Données à Caractère Personnel, ce que le Client reconnait et accepte expressément.

Plus généralement, les termes et conditions relatifs au traitement des Données à Caractère Personnel par la Société en sa qualité de sous-traitant sont définis en annexe du Bon de Commande.

4.4 Le Client, en sa qualité de responsable de traitement, garantit à la Société qu'il respecte les obligations lui incombant au titre des Lois et Réglementations sur la Protection des Données à Caractère Personnel, en particulier celles relatives aux Données de Santé et Données Biométriques.

A ce titre, le Client garantit la Société contre tout recours, plainte ou réclamation émanant d'une personne physique, dont les Données à Caractère Personnel, en particulier les Données de Santé et Données Biométriques qui seraient traitées dans le cadre du Contrat et qui résulterait d'un non-respect par le Client ou un tiers d'une des obligations au titre des Lois et Réglementations sur la Protection des Données à Caractère Personnel et/ou toutes dispositions légales et/ou réglementaires spécifiques aux Données de Santé.

En particulier, le Client garantit à la Société qu'il a obtenu le consentement, si nécessaire, de toutes les personnes physiques et qu'il les a dûment informées avant la collecte, le traitement, le stockage, l'utilisation et le partage de leurs Données à Caractère Personnel.

5- DÉCLARATIONS ET GARANTIES

5.1 Déclarations et garanties de la Société

Outre les garanties prévues aux Conditions Communes, la Société déclare et garantit que le Service Hébergement est fourni au Client selon les usages de la profession, les termes du Contrat, en particulier du SLA, et conformément aux Lois et Réglementations sur la Protection des Données à Caractère Personnel en vigueur et aux réglementations spécifiques applicables au traitement des Données de Santé et Données Biométriques le cas échéant.

5.2 Sauf stipulation contraire expresse du Contrat et dans la mesure autorisée par les dispositions légales applicables, toutes garanties, déclarations et/ou engagements de toute nature, exprès ou tacites, autres que ceux expressément prévu(s) au Contrat sont exclus.

5.3 Déclarations et garanties du Client

Le Client garantit qu'il dispose de tous les droits, notamment les Droits de Propriété Intellectuelle, utiles et nécessaires pour permettre l'exécution du Service Hébergement et permettant notamment au Client de transférer le Progiciel Tiers à la Société en vue de la réalisation de l'Hébergement.

Le Client déclare et garantit qu'il s'engage à respecter toutes les Lois et Règlementations sur les Données à Caractère Personnel en vigueur lors de la collecte, la compilation, le stockage, la consultation et le traitement de toute Donnée à Caractère Personnel utilisée dans le cadre du Service Hébergement, et de manière générale, à se conformer à toutes lois et réglementations applicables.

Le Client exonère expressément la Société de toute responsabilité médicale.

En outre, le Client est responsable (i) du choix du Service Hébergement, de son utilisation et des résultats obtenus, et du respect des conditions du Contrat par les Utilisateurs, et (ii) de tout dommage résultant d'une utilisation non autorisée ou non conforme du Service Hébergement et/ou de toute information inexacte ou incomplète fournie à la Société par le Client.

Le Client déclare avoir une bonne connaissance d'Internet, de ses caractéristiques et de ses limites. En particulier, le Client reconnaît que (i) la fiabilité technique de la transmission des données par Internet est relative, puisqu'elles circulent sur des réseaux hétérogènes dont les caractéristiques et les capacités techniques sont diverses, parfois surchargées et/ou susceptibles de présenter des dysfonctionnements ; (ii) l'Environnement Client est connecté au Data Center sous sa seule responsabilité ; (iii) que les données communiquées via Internet, y compris les Données, sans préjudice des moyens de protection existants mis en œuvre par la Société - peuvent être soumises à d'éventuels détournements ; (iv) certains réseaux spécifiques peuvent dépendre d'accords particuliers et être soumis à des restrictions d'accès. Compte tenu de la technicité des technologies mises en œuvre et de l'impossibilité de contrôler les réseaux connectés au réseau de la Société, cette dernière ne peut être en aucun cas responsable de la fiabilité des transmissions des Données, des temps d'accès, des éventuelles restrictions d'accès sur des réseaux et/ou serveurs spécifiques connectés au réseau Internet.

6- PROPRIETE INTELLECTUELLE

La Société et/ou ses concédants conservent la propriété de la Plateforme d'Hébergement, des logiciels associés, et de manière générale, de tous éléments mis à la disposition du Client et de toutes prérogatives s'y rattachant, aux fins d'exécution du Contrat et pour lesquels, la Société concède au Client, les droits personnels, non-exclusifs, révocables et non-transférables d'utilisation nécessaires à l'exécution du Contrat, pour ses besoins propres et pour la Durée du Contrat (y compris le cas échéant pendant la Phase de Réversibilité) ; la Société (et/ou ses concédants) conservant la propriété exclusive du Progiciel, ainsi que prévu par ailleurs dans les stipulations du Contrat applicables aux Licences et des résultats de tous travaux résultant des Prestations réalisées par la Société, notamment dans le cadre de la Phase Préparatoire.

Pour sa part, et le cas échéant, le Client concède à la Société les droits d'utilisation du Progiciel Tiers qu'il met à sa disposition dans le cadre de l'exécution du Contrat, pour la Durée et pour les seuls besoins de l'exécution du Contrat.

7- RESILIATION ET EFFETS DE FIN DE CONTRAT

7.1. Résiliation

Sans préjudice des causes de résiliation prévues dans le cadre des Conditions Communes, dans les Conditions Spécifiques afférentes à la Licence et le cas échéant, aux Services Maintenance et Assistance, il est prévu que chacune des Parties pourra également et de plein droit résilier le Service Hébergement par lettre recommandée avec demande d'avis de réception, sans mise en demeure préalable ni préavis, et sans qu'aucune indemnité ne soit due à l'autre Partie, dans le cas de fin de la Licence pour quelque cause que ce soit.

7.2. Effets de fin de Contrat

7.2.1 A la fin du Contrat, quelle qu'en soit la cause et sans préjudice des stipulations des Conditions Communes et le cas échéant des Conditions Spécifiques applicables à la Licence concernée et le cas échéant, aux Services Maintenance et Assistance :

- sous réserve des termes convenus pour la Phase de Réversibilité, la Société cesse immédiatement de fournir au Client le Service Hébergement ;

- dans le cas où le Progiciel en Mode Hébergé est un Progiciel Tiers, la Société s'engage à le restituer au Client ;

- le Client s'engage à procéder au paiement immédiat de toutes les sommes dues à la Société au titre du Contrat et ce, sans qu'il ne puisse être procédé à quelconque compensation ou déduction : les montants versés à la Société restant par ailleurs acquis à cette dernière, sauf stipulation expresse contraire du Contrat.

7.2.2 Le Client peut, moyennant une demande écrite, demander à la Société de lui restituer les Données telles qu'enregistrées à l'issue de la dernière sauvegarde effectuée au titre du Contrat, dans les conditions prévues à l'article 8 « Phase de Réversibilité » des présentes Conditions Spécifiques.

7.2.3 En outre, les articles 7 et 8 ainsi que toutes les stipulations ayant par nature vocation à survivre à l'expiration du Contrat, survivront à l'expiration ou à la résiliation du Contrat quelle qu'en soit la cause et conserveront leurs effets pour la durée qui sera nécessaire à leur donner l'effet prévu.

8- PHASE DE REVERSIBILITE

8.1 A la fin du Service Hébergement pour quelque cause que ce soit, et pour le cas où le Client confierait à un tiers ou reprendrait à son compte l'Hébergement, la Société s'engage à fournir toute Prestation d'assistance ou de conseil permettant de faciliter la réversibilité et maintenir dans la mesure du possible l'accessibilité du Progiciel, du Progiciel Tiers et des Données si le Client en fait la demande, et notamment à remettre au Client ou au prestataire tiers désigné par le Client, tous les éléments et informations dont elle dispose, afin d'éviter une rupture dans l'exploitation et l'accessibilité du Progiciel en Mode Hébergé et des Données.

Les opérations de réversibilité se déroulent pendant la durée nécessaire à la réalisation de la réversibilité. Les Prestations fournies par la Société au titre de la Phase de Réversibilité seront à la charge du Client, feront l'objet d'un Bon de Commande, et seront facturées aux tarifs en vigueur de la Société.

8.2 Le Client devra demander par écrit le démarrage de la Phase de Réversibilité au plus tard trente (30) Jours Ouvrés avant la date d'expiration du Contrat, ou dans un délai de trente (30) Jours Ouvrés suivant la fin du Service Hébergement, quelle qu'en soit la cause, la validité du Contrat et les obligations correspondantes des Parties étant maintenus pendant toute la période de réversibilité sous réserve du paiement des prix correspondants, laquelle cesse à la date de fin effective du Contrat ou du Service Hébergement.

Dans ce cas, et dans un délai de quinze (15) Jours Ouvrés à compter de la notification de la résiliation ou de la date de cessation du Contrat ou de la fin du Service Hébergement, les Parties se rencontreront en vue de définir les conditions de réalisation de la réversibilité, et en particulier un plan de réversibilité décrivant les modalités de reprise de l'exécution du Service Hébergement du Progiciel.

Le Client disposera alors d'un délai de quinze (15) Jours Ouvrés pour valider le plan de réversibilité ou proposer les amendements qu'il jugera nécessaires. Dans le silence du Client ou absence de demande de modification à l'issue de ce délai, le plan de réversibilité sera réputé accepté par les deux Parties.

Le Client désignera, par écrit et préalablement au démarrage effectif de la réversibilité, l'éventuel tiers qui sera chargé de reprendre le Service Hébergement.

8.3 La Société accepte dans ce cadre :

- de collaborer au cours de la Phase de Réversibilité organisée au profit de tout repreneur ou du Client sous réserve de la même collaboration de la part de ce repreneur et du Client ;
- d'assurer les opérations de réversibilité conformément au plan de réversibilité qui aura été défini en concertation entre les Parties ;
- de continuer à fournir, pendant la Phase de Réversibilité, le Service Hébergement selon les conditions et modalités définies au Contrat moyennant le paiement du prix correspondant.

Le Client s'engage quant à lui à :

- assurer l'organisation et la coordination des différentes tâches associées à la réversibilité ;
- affecter des équipes compétentes à la reprise du Service Hébergement ;
- à régler toutes factures émises par la Société au titre du Service Hébergement ;

8.4 Le Client déclare avoir été informé et avoir accepté que le bon déroulement du plan de réversibilité dépend pour une grande part des moyens techniques et humains mis en œuvre par le Client et / ou le tiers désigné par le Client. En aucun cas, la Société ne pourra être tenue de réaliser une prestation qui serait la conséquence de la défaillance du Client et / ou du tiers désigné par le Client, ou de l'insuffisance des moyens mis en œuvre par le Client ou le tiers désigné par le Client.

La restitution des Données fera l'objet d'un procès-verbal signé par les deux (2) Parties. Au- delà du délai de trente (30) Jours Ouvrés susvisés et sous réserve de toute disposition légale ou réglementaire applicable, la Société est autorisée à supprimer de la Plateforme d'Hébergement toute les Données.

9-AUDIT

9.1 Sous réserve des stipulations spécifiques au traitement des Données à Caractère Personnel, les Parties conviennent que le Client pourra, après en avoir avisé la Société par écrit et avec un préavis minimum de trente (30) Jours Ouvrés, faire procéder à ses frais, au maximum une (1) fois par an, et au plus tôt six (6) mois après le début du Contrat, à un audit visant à vérifier le respect de ses principaux engagements contractuels liés aux conditions de réalisation du Service Hébergement par la Société.

L'audit pourra être réalisé soit par les auditeurs internes du Client, soit par un cabinet extérieur, qui ne pourra en aucun cas être un concurrent de la Société. Le Client doit notifier à la Société l'identité de la structure d'audit retenue lorsqu'il s'agit d'un cabinet extérieur.

9.2 Le démarrage de la mission sur le site de la Société se fera selon les modalités et aux dates définies dans un planning d'audit établi en concertation entre l'auditeur et l'interlocuteur privilégié de la Société.

9.3 Les auditeurs devront en tout état de cause prendre à engagement formel de confidentialité et de non-divulgation. Les auditeurs s'engageront notamment dans ce cadre, à (i) respecter les règles de fonctionnement et de sécurité en vigueur chez la Société, (ii) ne rien faire qui puisse porter atteinte à la bonne exécution du Service Hébergement par la Société et plus généralement perturber les activités de l'entreprise, et à (iii) conserver confidentielles toutes informations dont ils viendraient à prendre connaissance à l'occasion de la réalisation de l'audit.

9.4 Dans le cadre de cet audit, la Société s'engage à coopérer avec les auditeurs de bonne foi, et à leur fournir toutes les informations nécessaires dans la mesure où ces informations ne concernent pas des points confidentiels d'éléments mutualisés. Le temps passé par le personnel de la Société à assister les auditeurs donnera lieu à facturation en fonction des conditions tarifaires en vigueur et du profil et du niveau d'expérience des intervenants de la Société.

9.5 L'audit ne pourra concerner la partie du Service Hébergement sous-traitée que dès lors que les sous-traitants auront autorisé l'audit et le plan d'audit qui leur aura été soumis.

9.6 Les rapports d'audit seront gratuitement adressés à la Société et feront l'objet d'un examen lors d'une réunion entre les Parties. Au cas où, suite à cet examen, un rapport d'audit ferait apparaître une infraction substantielle aux obligations de la Société visées au Contrat, cette dernière s'engage à mettre en œuvre, à ses frais, l'ensemble des mesures correctives nécessaires dans un délai défini d'un commun accord entre les Parties, pour y remédier.

Si les conclusions de certains audits contiennent des recommandations tendant à la modification ou à l'amélioration des règles et procédures auditées, la mise en œuvre de ces recommandations pourra s'effectuer par voie d'avenant, et selon les tarifs de la Société.

10- EVOLUTION TARIFAIRES DES FOURNISSEURS

Sans préjudice des dispositions de l'article 29 des Conditions Communes, le Client reconnaît et accepte que les prix relatifs au Service Hébergement définis au Contrat peuvent être soumis à des modifications, en cas d'évolutions tarifaires importantes chez les fournisseurs de la Société, tels que les fournisseurs d'hébergement, lesquelles modifient alors substantiellement l'économie du Contrat. La Société peut alors refléter ces évolutions dans ses propres tarifs, et notifie le Client par lettre recommandée avec demande d'avis de réception des nouveaux prix applicables, au moins un (1) mois avant leur prise d'effet. A compter de cette notification écrite, le Client dispose de dix (10) Jours Ouvrés pour s'opposer par écrit à cette modification. Pendant cette période prolongée de cinq (5) Jours Ouvrés, les Parties pourront se concerter, et à défaut d'accord, chacune des Parties pourra mettre fin au Service Hébergement à l'issue de la période annuelle en cours – étant précisé que les prix sont alors inchangés pour la période annuelle restant à courir. Passé le délai de dix (10) Jours Ouvrés susvisé, et en l'absence d'objection écrite du Client, la modification tarifaire sera réputée acceptée par le Client et deviendra automatiquement applicable.

Addendum 1 – Prérequis Techniques ; Description du Service Hébergement ; Niveaux de Service (« SLA »)

1. Prérequis Techniques

Les Prérequis Techniques sont décrits dans le Bon de Commande correspondant.

2. Description du Service Hébergement

2.1 Phases contractuelles

- **Phase Préparatoire**

La Phase Préparatoire a pour objet essentiel de permettre :

- à la Société, de :

  - réaliser - en collaboration avec le Client et conformément au Contrat, les opérations nécessaires, le cas échéant, à la transposition du Progiciel, des Données, du Progiciel Tiers le cas échéant, vers la Plateforme d'Hébergement, en vue de sa prise en charge dans le cadre du Service Hébergement ;
  - parfaire sa connaissance de l'Environnement Client et constituer une base de connaissances y afférente ;
  - mettre en place la Plateforme d'Hébergement ;
  - définir et mettre en place, une organisation technique et humaine compatible avec ses engagements contractuels ;
  - débuter la fourniture du Service Hébergement, et

- au Client, de :

  - contrôler la conformité de la fourniture du Service Hébergement à ses besoins tels qu'exprimés dans le Contrat.

Les Parties conviennent que la Société n'est pas encore tenue par les engagements de Niveaux de Service pendant la Phase Préparatoire, et ce en raison de la nature même de ladite Phase.

La Société informe le Client, par courriel à l'adresse indiquée au Bon de Commande, de l'accessibilité du Service Hébergement. Par accessibilité, il convient d'entendre la possibilité par l'administrateur tel que visé à l'article 3.2.2 des présentes, d'accéder au Progiciel en Mode Hébergé et ce, à partir de l'Environnement Client.

A compter de la date d'information relative à l'accessibilité du Service de l'Hébergement, le Client dispose d'un délai de cinq (5) Jours Ouvrés pour procéder aux deux (2) validations prévues par la présente annexe. En cas de problème(s) technique(s) relatif(s) à l'accessibilité pendant la période de validation susvisée, le Client s'engage à informer sans délai et par écrit la Société des problèmes constatés, présentés de manière aussi détaillée que possible. Toute réserve du Client devra être dument motivée et détaillée.

La Société s'efforce de résoudre le(s)dit(s) problème(s) et informe par écrit le Client de l'accessibilité du Service Hébergement, le Client disposant alors d'un nouveau délai de cinq (5) Jours Ouvrés pour procéder à nouveau aux deux (2) validations susvisées.

A l'issue de la période de recette de la Phase Préparatoire, si le Client n'a émis aucune contestation écrite relative à l'accessibilité du Service Hébergement, les Parties conviennent expressément que la Phase Préparatoire sera réputée recettée et le démarrage de la Phase de Production sera prononcé.

De convention expresse, seuls les problèmes constatés lors de la phase initiale de recette seront pris en compte lors de la seconde phase éventuelle de recette.

Dans le cas où les problème(s) signalé(s) sont de la responsabilité du Client, la Société peut refacturer au Client le temps passé par ses équipes à résoudre le(s)dits problème(s), au tarif en vigueur au moment de l'intervention ainsi que les frais corrélatifs engagés par la Société.

En tout état de cause, toute connexion au Progiciel en Mode Hébergé sur la Plateforme d'Hébergement par un ou plusieurs Utilisateurs vaut recette irrévocable et sans réserve du Service Hébergement.

- **Phase de Services Régulier**

La Phase de Production démarre à l'issue de la Phase Préparatoire, et ce dès le prononcé de la recette.

A compter du démarrage de la Phase de Production, la Société est tenue de fournir le Service Hébergement conformément aux Niveaux de Service.

La Société peut modifier à sa convenance les moyens et ressources mis en œuvre pour fournir le Service Hébergement, sous réserve que cela n'impacte pas de manière négative la qualité des services fournis.

2.2 Sauvegarde des Données

La Société met en place une stratégie de sauvegarde des Données. Une sauvegarde quotidienne des Données est réalisée sept (7) jours sur sept (7). Cette sauvegarde est incrémentale (seules sont enregistrées les modifications de la journée). Les sauvegardes sont conservées pendant un délai de quatre (4) semaines.

Une copie de sauvegarde est entreposée dans le Data Center de secours.

En cas d'Anomalie nécessitant l'utilisation de ces sauvegardes, les obligations de la Société sont exclusivement les suivantes :

- recherche de la sauvegarde la plus récente des Données,
- installation et remise en production de cette sauvegarde.

Il appartient au Client de mettre en œuvre des mesures de nature à assurer la continuité du service pour lequel le Progiciel en Mode Hébergé est utilisé en cas d'inaccessibilité absolue du Data Center.

3. Niveaux de Service

La présente clause décrit :

- les Niveaux de Service, les engagements de disponibilité et les garanties de temps de prise en compte ;
- les mesures de performance de ces indicateurs permettant d'évaluer le respect des engagements de la Société.

3.1 Disponibilité du Service

L'Hébergement est accessible vingt-quatre (24) heures sur 24 et sept (7) jours sur 7, hors plages d'indisponibilité pour les causes décrites ci-après.

La Société garantit une disponibilité moyenne annuelle de **99,5 %** du Service.

Le taux de disponibilité est calculé en soustrayant de 100% des heures mesurables au cours de la période annuelle concernée, toute indisponibilité non due à/au :

(i) un arrêt autorisé par le Client ou à la demande du Client ;
(ii) à la maintenance programmée ou la maintenance exceptionnelle ou d'urgence telles que visées au 3.2 de la présente annexe, et aux articles 3.3 et 3.4.2.
(iii) à un des cas visés aux exclusions décrites à l'article 3.6.

3.2 Maintenance programmée ; maintenance exceptionnelle ou d'urgence

La Société peut restreindre ou suspendre la fourniture du Service Hébergement - sans indemnité et sans préjudice des sommes dues au titre du Contrat dans les cas suivants :

- **Maintenance programmée** : toute interruption du Service Hébergement au titre de la maintenance programmée devra être signalée par courriel au Client, moyennant – dans la mesure du possible et sauf urgence – un préavis de cinq (5) Jours et a minima de quarante-huit (48) heures notifié par courriel.
  Le Client reconnait et accepte que la période de maintenance programmée puisse temporairement rendre le Service Hébergement inaccessible.
  De convention expresse, l'indisponibilité du Service Hébergement au titre de la maintenance programmée sera dans la mesure du possible programmée par la Société aux moments de la journée les moins préjudiciables pour le Client ;

- **Maintenance exceptionnelle ou d'urgence** : la Société pourra procéder, sans contrainte de plage horaire, à des maintenances, mises à jour et/ou évolutions exceptionnelles avec une indisponibilité totale ou partielle de service de quatre (4) heures ouvrées consécutives au maximum, dans le cas visé à l'article 3.4.2 des Conditions Spécifiques et/ou pour anticiper un problème important (faille de sécurité, virus…) ou effectuer une opération curative ou réglementaire, Dans la mesure du possible et sauf urgence, la Société en informera le Client, vingt-quatre (24) heures à l'avance par une notification électronique (mail).

3.3 Signalement des Anomalies

Toute Anomalie suspectée doit être signalée par les interlocuteurs techniques du Client au service support de la Société via l'outil ticketing.

L'interlocuteur technique doit disposer de connaissances techniques suffisantes pour pouvoir échanger utilement avec le support. Il doit également avoir les pouvoirs suffisants pour pouvoir engager le Client.

Le Client doit accompagner chacune de ses requêtes au titre du signalement des Anomalies, d'une description détaillée et documentée de l'Anomalie rencontrée et de l'incidence sur le fonctionnement du Progiciel en Mode Hébergé.

Le Client s'engage à participer activement à la correction des Anomalies en communiquant notamment à la Société tout document et/ou toute information que la Société estime raisonnablement nécessaire(s).

Toute demande adressée au support technique pour une difficulté d'utilisation du Service Hébergement ne constituant pas une Anomalie, et en particulier non imputable à la Société ou ne relevant pas du présent Contrat, pourra faire l'objet d'une facturation additionnelle.

3.4 Délai de prise en compte

La Société garantit un délai de prise en compte de quatre (1) heure ouvrée.

3.5 Mesures des délais de prise en compte

Le délai de prise en compte commence à courir lorsque la Société a été informée de l'Anomalie par l'interlocuteur technique, conformément aux stipulations du Contrat.

Le délai de prise en compte ne commence à courir que sous réserve de la communication par le Client de l'ensemble des informations et éléments requis par la Société dans ce cadre.

Un tableau de bord annuel représentant les mesures enregistrées des délais de prise en compte pourra être mis à la disposition du Client si celui-ci en fait la demande.

3.6 Exclusions

La Société est exonérée de toute obligation au titre de la présente annexe dans les cas suivants :

- interruptions ou dégradations du Service Hébergement lorsque celles-ci résultent des hypothèses d'indisponibilité du Service d'Hébergement telles que notamment formulées au 3.2 de la présente annexe ;
- interruptions ou dégradations de Service Hébergement qui seraient du fait du Client, et notamment de son propre système et ses propres machines, liées à la mise à jour et/ou évolution constante de ses logiciels et ses matériels ou à une autre opération de maintenance ;
- interruptions ou dégradations du Service Hébergement liés à des erreurs du Progiciel Tiers, à un mauvais paramétrage applicatif ou à une erreur de manipulation affectant la base de données ;
- interruptions ou dégradations du Service Hébergement n'entrant pas dans les engagements de la Société ;
- interruptions ou dégradations du Service Hébergement qui seraient du fait du réseau des perturbations des réseaux de télécommunication ou du propre système du Client et liées à tout événement extérieur à la Société, mettant cette dernière dans l'impossibilité de fournir le Service Hébergement ;
- difficultés d'accessibilité ou impossibilité momentanée du Service Hébergement et/ou du Progiciel en Mode Hébergé dus à un cas de force majeure ou hors du contrôle de la Société.

Addendum 2 - Plan Assurance Sécurité

(Extrait)

Le plan d'assurance sécurité informe et reprend les mesures organisationnelles et techniques du MiPih pouvant être mise en œuvre dans le cadre de l'infogérance en hébergement d'un système d'information ou de tout système d'information pouvant adresser des données de santé.

1. ***Hébergeur de données de Santé (HDS)***

Le MiPih est certifié HDS par l'AFNOR pour 3 ans depuis le 28 aout 2018 en tant que :

- HEBERGEUR D'INFRASTRUCTURE PHYSIQUE
- ET HEBERGEUR INFOGEREUR.

Pour les prestations « HEBERGEMENT D'INFRASTRUCTURE PHYSIQUE ET HEBERGEMENT AVEC INFOGERANCE TECHNIQUE ET APPLICATIVE CONCERNANT DES DONNEES DE SANTE A CARACTERE PERSONNEL ».
Auparavant le MiPih était agréé hébergeur de données de santé pour le même périmètre depuis le 4 janvier 2012.

afaq
AFNOR CERTIFICATION

Certificat
Certificate

N° 2018/80283.8 — **Page 1 / 1**

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

MIPIH

pour les activités suivantes :
for the following activities:

HEBERGEUR D'INFRASTRUCTURE PHYSIQUE ET HEBERGEUR INFOGEREUR

1. LA MISE A DISPOSITION ET LE MAINTIEN EN CONDITION OPERATIONNELLE DES SITES PHYSIQUES PERMETTANT D'HEBERGER L'INFRASTRUCTURE MATERIELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMENT DES DONNEES DE SANTE
2. LA MISE A DISPOSITION ET LE MAINTIEN EN CONDITION OPERATIONNELLE DE L'INFRASTRUCTURE MATERIELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMENT DE DONNEES DE SANTE
3. LA MISE A DISPOSITION ET LE MAINTIEN EN CONDITION OPERATIONNELLE DE LA PLATEFORME D'HEBERGEMENT D'APPLICATIONS DU SYSTEME D'INFORMATION
4. LA MISE A DISPOSITION ET LE MAINTIEN EN CONDITION OPERATIONNELLE DE L'INFRASTRUCTURE VIRTUELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMENT DES DONNEES DE SANTE
5. L'ADMINISTRATION ET L'EXPLOITATION DU SYSTEME D'INFORMATION CONTENANT LES DONNEES DE SANTE
6. LA SAUVEGARDE DE DONNEES DE SANTE

DECLARATION D'APPLICABILITE Version 1.4 DU 22 FEVRIER 2021.
GIP MIPIH - MIDI PICARDIE INFORMATIQUE HOSPITALIERE est certifié selon l'ISO/IEC 27001:2013.

a été évalué et jugé conforme aux exigences requises par :
has been assessed and found to meet the requirements of:

REFERENTIEL DE CERTIFICATION HDS 1.1 - Juin 2018

et est déployé sur les sites suivants :
and is developed on the following locations:

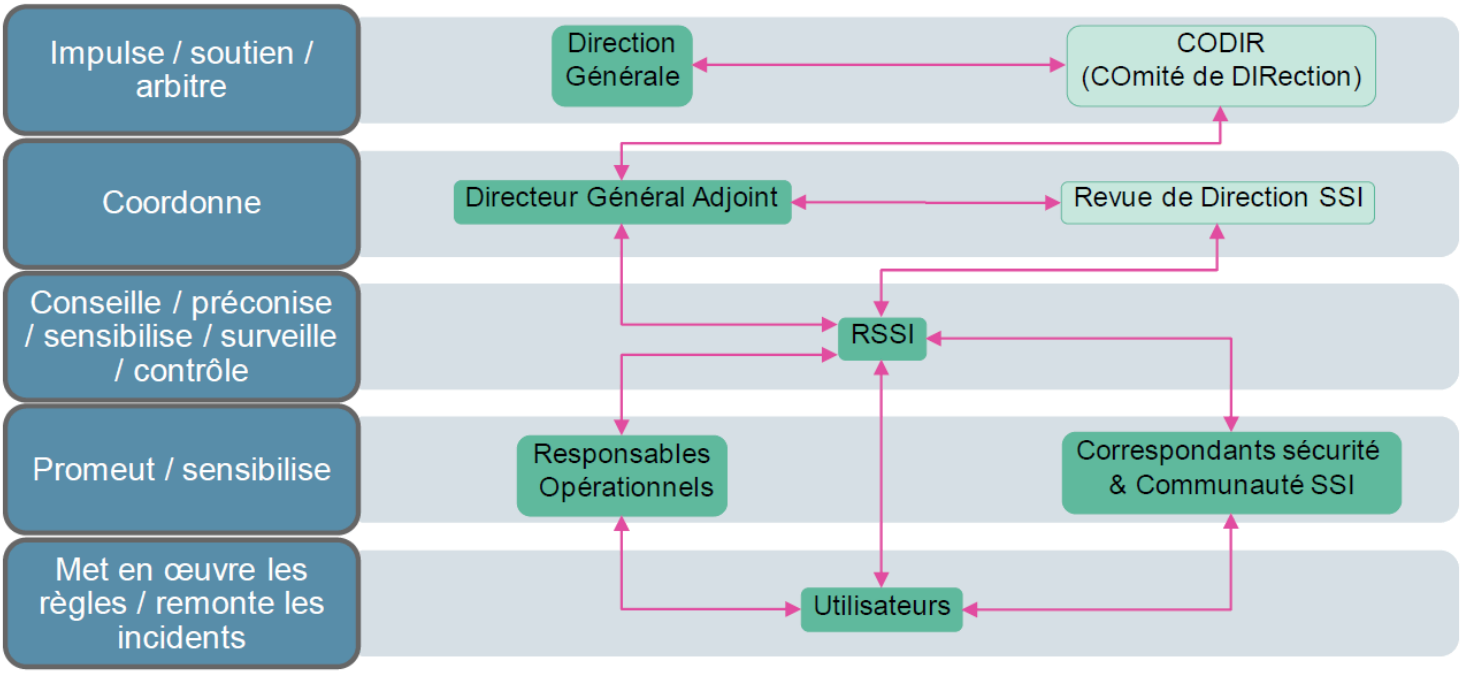
12 RUE MICHEL LABROUSSE FR-31036 TOULOUSE CEDEX 1
2 BIS IMPASSE MICHEL LABROUSSE FR-31036 TOULOUSE CEDEX 1
45 BOULEVARD AMBROISE PARE FR-80000 AMIENS

Ce certificat est valable à compter du (année/mois/jour) *This certificate is valid from (year/month/day)* **2021-08-28** Jusqu'au *Until* **2024-08-27**

Julien NIZRI
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification

2. ***Organisation liée à la sécurité des systèmes d'information***

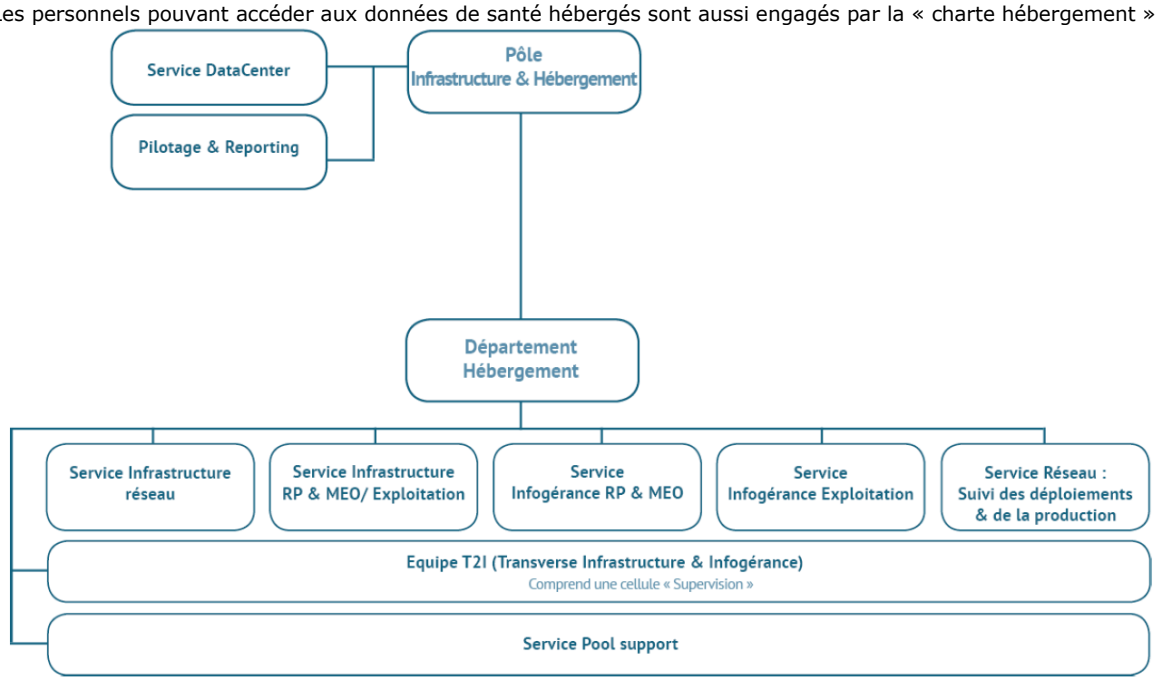
La sécurité des systèmes d'informations (SSI) est sous la responsabilité de deux Responsable Sécurité des Systèmes d'Information (RSSI) et d'un Revue de Direction SSI.



Les fonctions de contrôles sont assurées, sous couvert de la direction générale, par les responsables Qualité, Sécurité et par le médecin de l'hébergeur.

3. ***Le personnel hébergeur***

L'activité hébergement dépend d'un pôle dédié « Hébergement et infrastructure ».
Le contrat de travail des personnels engagés par le MiPih fait apparaître l'engagement du contractant au secret professionnel.
Les personnels pouvant accéder aux données de santé hébergés sont aussi engagés par la « charte hébergement ».



Les équipes du pôle « Infrastructure & Hébergement » sont dédiées à l'Hébergement.

Les équipes « Infrastructure Réseau » et « Réseau : Suivi des déploiements et de la production » gèrent le maintien en conditions opérationnelles et la supervision de l'ensemble des équipements réseau et sécurité du MiPih, LAN & WAN. Ces

équipes gèrent également la mise en place des nouveaux équipements et des liaisons réseaux des sites hébergés et autonomes (avant-vente des offres réseaux MiPih, suivi du déploiement, suivi des clients en production).

L'équipe « Infrastructure RP&MEO / Exploitation» gère en mode projet la mise en place de l'infrastructure nécessaire au passage en hébergement de nouvelles applications (gestion de projet, travail collaboratif avec le service informatique des adhérents pour mise en place de l'infogérance, coordination avec les éditeurs, mise à disposition de l'infrastructure).

L'équipe « Infogérance RP&MEO » gère les projets de reprise en hébergement des applications MiPih et les projets de démarrage. Ces équipes gèrent également la mise en place des flux de Tiers de télétransmission.

L'équipe « Infogérance Exploitation» gère les évènements issus de la supervision (GDS) et des traitements ordonnancés (GTO). Elle est responsable de la gestion du changement (GDC) autour des montées en version applicatives des produits MiPih (Agirh, Pastel, Magh2, QI …) – Offre d'Infogérance Applicative. Elle contribue à la gestion des incidents (GDI)

L'équipe « T2I – Transverse Infrastructure et Infogérance» participe à la définition des nouvelles infrastructures, a en charge leur mise en oeuvre et leur maintien en condition Opérationnelle. Elle contribue également en niveau « expertise » au Support

Le « Pool Support » assure le Niveau 1 & 2 des incidents techniques et réalise les demandes de travaux.

3.1. Les engagements du personnel

3.1.1 Contrat de travail

Le contrat de travail des personnels engagés par le MiPih fait apparaître l'engagement du contractant au secret professionnel le plus absolu.

3.1.2 Habilitation hébergement

Un engagement spécifique est demandé aux personnels habilités à accéder aux environnements hébergeant des données de santé dans le cadre de leur mission.

3.1.3 Charte de bon usage

Les personnels pouvant accéder aux données de santé hébergés sont aussi engagés par la « charte hébergement ».

3.2 Organisation du pôle Hébergement

L'infogérance a pour objet d'assurer en toute sécurité pour les établissements de santé et leurs patients, l'hébergement et/ou l'exploitation et le support de services applicatifs de tout ou partie de leur SIH, ceci incluant des applications gérant des données de santé.

Cette activité est gérée au MiPih par le Pôle « Hébergement » et est répartie sur les deux sites géographiques de Toulouse et d'Amiens.

Les activités clés concernant l'infogérance se répartissent selon les thèmes suivants :

- L'hébergement d'application, qui met à disposition des établissements une infrastructure d'hébergement pour leurs applications (locaux, matériel informatique, environnement logiciel) complète, redondante et sécurisée.

- Le support à l'infogérance, qui au travers du Centre de Support Hotline, prend en charge les demandes de travaux, traite les Incidents en intervenant si besoin sur les données, les traitements, les flux ou l'infrastructure, en liaison avec les supports fonctionnels applicatifs.

L'organisation du pôle distingue les activités suivantes :

- L'Infogérance et l'exploitation des services hébergés,
- Support des infrastructures internes et des infrastructures dédiées à l'hébergement,
- La Sécurité des systèmes d'information.

Le bon fonctionnement du Système d'Information du MiPih, ainsi que l'infrastructure dédiée à l'hébergement des Systèmes d'Information des établissements info-gérés, s'appuie sur une infrastructure composée de :

- un centre de traitement informatique principal et un de secours distant (réplication de données, reprise d'activité) sécurisés (intrusions, incendie, supervision),
- des serveurs et baies de disque dédiés aux applications info-gérées, associés à des environnements logiciels adaptés (OS, SGBD, outils),
- une interconnexion réseau sécurisée entre les établissements et le MiPih (via le service complémentaire Adhermip) et une connectivité à Internet.

Il en résulte les activités suivantes :

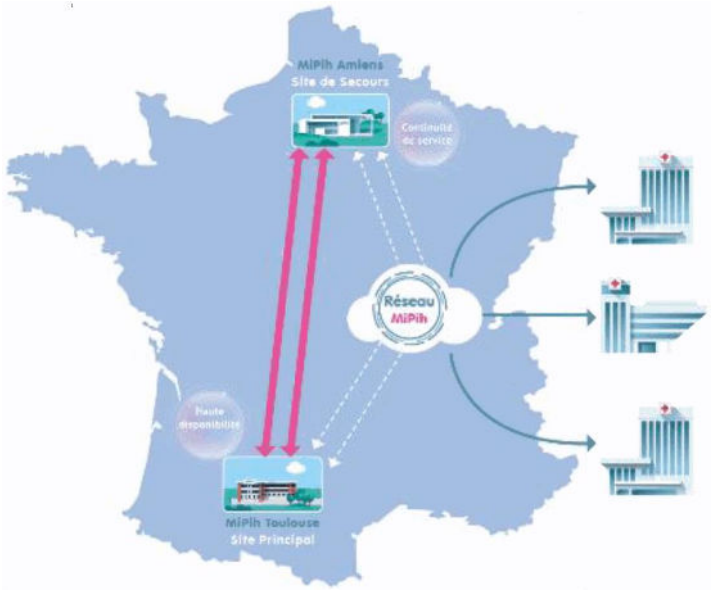
- Administration et supervision de l'infrastructure, Sauvegardes centralisées, Support aux « services »,
- Centre d'appel et gestion des Incidents des utilisateurs internes,
- Gestion des problèmes liés à l'infrastructure, y compris celle dédiée à l'infogérance hébergée,
- Gestion des changements (matériel, logiciel), suivi des configurations.

4. ***Sécurité physique***

Un service spécialisé dans l'hébergement et l'infogérance de traitements du système d'information hospitalier est proposé aux adhérents. Une organisation et des moyens techniques ont été mis en place pour répondre à des exigences de performance et de sécurité notamment pour assurer une continuité des activités essentielles (hébergement, infogérance et exploitation, paie, support). Les locaux géographiquement distants se répartissent en une infrastructure de production à Toulouse et le secours à Amiens.

Le MiPih met en oeuvre des moyens techniques adaptés. Pour cela il dispose de deux « Datacenter » hautement sécurisés distants de 900 km l'un à Toulouse (site principal), l'autre à Amiens (site de secours).

- 12 rue Michel Labrousse à Toulouse (site nominal).
- 43 av d'Italie à Amiens (site de secours).



Les caractéristiques relatives à la sécurité physique des Datacenter sont les suivantes :

- Services généraux :
  - qualité et continuité de la fourniture d'énergie,
  - sécurité de la climatisation,
  - qualité du câblage,
  - protection contre la foudre,

- Aux contrôles d'accès aux locaux sensibles,
  - gestion des droits et des autorisations d'accès aux locaux sensibles,
  - détection des intrusions,
  - surveillance des locaux sensibles,
  - contrôle d'accès au câblage
  - localisation des locaux sensibles

- À la sécurité contre les dégâts des eaux,
  - Prévention des risques de dégâts des eaux
  - Détection des dégâts des eaux
  - Evacuation de l'eau

- À la sécurité contre l'incendie,
  - Prévention des risques incendie,
  - Détection incendie,
  - Extinction incendie
- À la protection contre les risques environnementaux.

4.1 Accès aux locaux

L'accès à l'ensemble des locaux est contrôlé à l'aide d'un système centralisé pour les sites de Toulouse et d'Amiens. Les accès se font par badge. Chaque agent dispose d'un badge nominatif lui permettant l'accès aux bâtiments. Certains secteurs des bâtiments, soumis à autorisation, obligent à une nouvelle authentification. C'est le cas des zones sensibles tels que les locaux techniques et des salles informatiques qui ne sont accédés que par du personnel identifié et autorisé. Les entrées et sorties sont systématiquement enregistrées. Des badges « fournisseurs », réservés aux interventions des sociétés extérieures (installations de matériel, maintenances) sont attribués sur demande formalisée.

4.1 Surveillance des bâtiments

Les locaux du MiPih sont surveillés 24 heures sur 24, 7 jours sur 7 par un système de contrôle d'intrusion et par la présence d'un gardien. Le bâtiment est sous alarme en dehors des heures de bureau. En cas d'alarme la société de surveillance informe une liste de personne prédéfinie pour la levée de doute. Tout incident fait l'objet d'un rapport.

4.2 Surveillance Data Center

Les Data Center du MiPih sont surveillés 24 heures sur 24, 7 jours sur 7 par les personnels de l'équipe « DataCenter ». La personne d'astreinte est en capacité de :

- Recevoir les alarmes transmises par les équipements en défaut,
- Appliquer la procédure adaptée à l'incident,
- Contrôler et intervenir à distance si possible,
- Intervenir sur site en cas d'incident nécessitant un déplacement.

Tout incident constaté fait l'objet d'un rapport.

L'astreinte porte notamment sur les points suivants :

- Détection d'eau,
- Alarme onduleur,
- Alarme température,
- Alarme incendie,
- Alarme climatisation

4.3 Site Principal

Le Datacenter de ce site dispose d'une surface globale de 800 m2 répartie sur 2 niveaux :

- Une partie en sous-sol de 500 m2 comportant la salle informatique, les galeries techniques de climatisation, le local opérateur et les locaux divers (préparation, extinction incendie).
- Une partie en RDC de 330 m2 hébergeant l'ensemble des locaux techniques.

Le niveau de continuité de services est de type Tier III+ 2N ce qui correspond à une disponibilité statistique de 99,982% ou une indisponibilité d'environ 1,6 heure par an des chaînes électriques et climatiques.

Les caractéristiques techniques mises en œuvre sont les suivantes :

- Sécurité incendie,
  - Détection incendie,
  - Extinction automatique au gaz neutre Argo 55

- Détection d'eau,
  - Câbles détecteurs hydro-sensibles en faux planchers
  - Centrale de détection de fuite multi zone

- Contrôles d'accès physique au bâtiment
  - Contrôle anti-intrusion : Les entrées et sorties sont contrôlées par un système à badge sans clavier (22 lecteurs)
  - Vidéosurveillance : 45 caméras

- Sécurité électrique :
  - Redondance totale des productions d'énergie, et interventions de maintenance transparentes sans interruption de service.
  - Groupe électrogène 100 heures d'autonomie sans réapprovisionnement
  - Onduleurs redondés puissance 500kVA autonomie 10 minutes à pleine charge

- Climatisation :
  - Climatisation de la salle informatique et du local opérateur.
  - Climatisation des locaux électriques

  Chaque production de froid est assurée par un refroidisseur de liquide à condensation par eau.

- Gestion Technique Centralisée (GTC)

Un système de gestion technique centralisé (GTC) permet de superviser et d'exploiter les informations ou alarmes remontées par les différents équipements (électricité, climatisation, détection d'eau, vidéo surveillance…). Ce système permet d'établir des historiques de fonctionnement et des tableaux de bord.
Cette centrale dédiée aux locaux informatiques est reliée au même type de centrale située sur le site de secours à Amiens.

4.4 Site de secours

La surface globale de ce Datacenter est d'environ 250 m², réparti ainsi :

- Une salle informatique de 120m²,
- Le reste de la surface est réparti en galeries techniques de climatisation, un local Opérateur et des locaux divers (extinction, …).

Le Niveau de continuité de service est de type Tiers III+ en 2N correspondant à une disponibilité statistique de 99,982% soit 1,6 heure d'indisponibilité annuelle.

Le site de secours d'Amiens dispose d'une sécurisation analogue à celle du site de Toulouse.

Les caractéristiques techniques mises en œuvre sont les suivantes :

- Sécurité Incendie
  - Détection incendie,
  - Extinction automatique au gaz neutre Argo 55

- Détection d'eau
  - Câbles détecteurs hydro-sensibles en faux planchers
  - Centrale de détection de fuite multi zone

- Contrôles d'accès – Anti-intrusion
  - Contrôle anti-intrusion : Les entrées et sorties sont contrôlées par un système à badge sans clavier (7 lecteurs)
  - Vidéosurveillance : 31 caméras

- Sécurité électrique
  - Redondance totale des productions d'énergie, et interventions de maintenance transparentes sans interruption de service.
  - Groupe électrogène 100 heures d'autonomie sans réapprovisionnement
  - Onduleurs redondés puissance 160kVA

- Climatisation
  - Climatisation de la salle informatique et du local opérateur.
  - Climatisation des locaux électriques

  Chaque production de froid est assurée par un refroidisseur de liquide à condensation par eau.

- Gestion Technique Centralisée (GTC)

Un système de gestion technique permet de superviser et d'exploiter les informations ou alarmes remontées par les différents équipements (électricité, climatisation, détection d'eau, vidéo surveillance). Cette centrale dédiée aux locaux informatiques est reliée à la centrale du site de Toulouse.

4.5 L'Infrastructure technique générale

Le MiPih dispose pour l'ensemble de ses activités d'une infrastructure matérielle sécurisée. Elle se compose de quatre ensembles distincts dont les équipements sont adressés sur 4 réseaux différents. Les échanges entre ces ensembles sont contrôlés par des pare feux. Néanmoins les équipements réseaux et ceux dédiés à la sauvegarde sont mutualisés entre les besoins internes et les services hébergés.

4.6 L'infrastructure hébergement

Elle est séparée des activités internes du MiPih, par un cloisonnement physique et logique. Elle est adressée sur un réseau dédié composé aussi de serveurs de type annuaire, serveurs d'application, serveurs de fichiers reliés à son propre réseau de stockage. La réplication des données entre les sites est de type asynchrone. Les données sont répliquées entre les baies SAN, la mise à jour est automatique. Seuls les blocs modifiés sont réécrits sur les baies de secours. Ce mécanisme de réplication est paramétrable par l'administrateur SAN. Les volumes échangés permettent une fréquence de réplication de 10 minutes entre les baies nominales et secours. Les durées maximales d'interruption des services hébergés sont inférieures à 4 heures. Les moyens mis en œuvre sur le site de secours sont dimensionnés en conséquence pour permettre la continuité des services hébergés sans dégradation de performance. Pour ce faire, le client doit avoir opté pour la réplication des données sur le site de secours.

4.7 Le réseau des « Adhérents » du MiPih

Les accès entre les établissements de santé et le MiPih se font au travers du réseau privé « Adhermip ». Les équipements nominaux permettant le routage des flux sont doublés sur le site de secours.

4.8 Les sauvegardes

4.8.1 L'Infrastructure de sauvegardes

Le MiPih dispose d'une infrastructure de sauvegarde. L'administration du système est sous la responsabilité du pôle Hébergement. Les opérations de sauvegarde ou de restauration sont réalisées par une équipe habilitée. Les opérations suivantes sont effectuées :

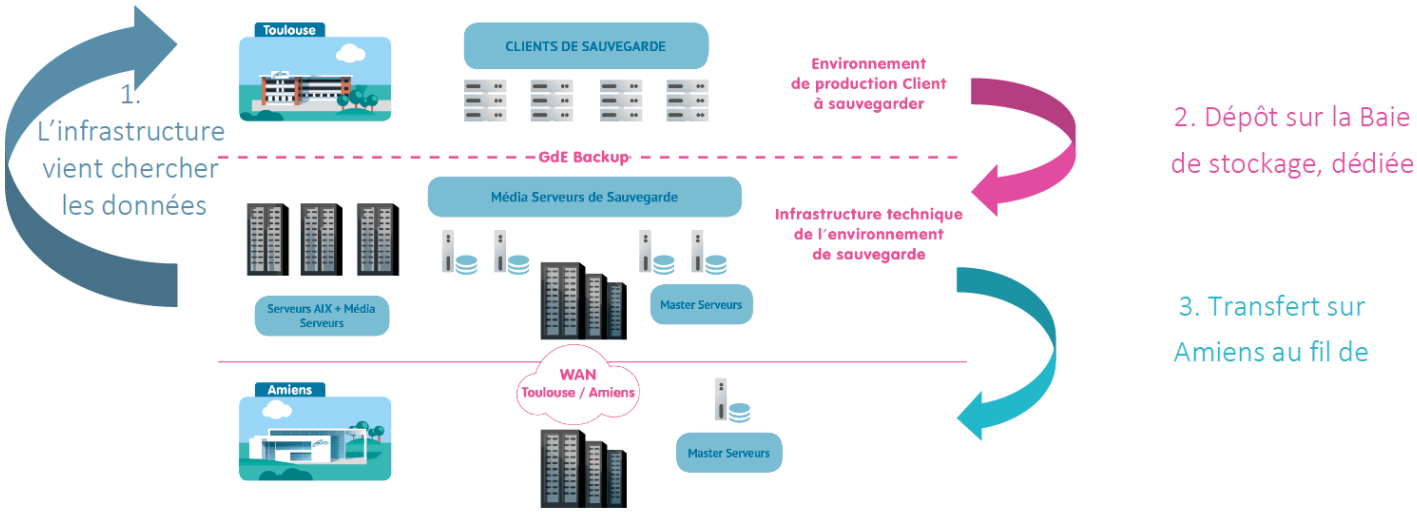
- Sauvegarde incrémentale et quotidienne des données des utilisateurs internes et des établissements hébergés. Quatre semaines de rétention.
- Sauvegarde hebdomadaire de l'ensemble des systèmes des serveurs. Quatre semaines de rétention.
- Externalisation sur site distant.

L'infrastructure de sauvegarde est répartie sur le site nominal et le site de secours. Elle est composée de :

- des serveurs hébergeant les logiciels de sauvegarde,

- des serveurs dédiés à la déduplication (procédé consistant à ne copier qu'une fois les données sur disque physique un même bloc provenant de serveurs différents),
- deux baies de disques (Data Domain). Une première sur le site principal et une deuxième sur site de secours,

Les serveurs assurant les processus de sauvegarde sont placés dans un même pool de serveur. La sauvegarde est lancée sur la machine la moins sollicitée (équilibrage de charge).



4.8.2 La Politique de sauvegarde

Les données « hébergées» sont sauvées sur une baie de disque et dupliquées sur une baie distante sur le site de secours. Elles sont conservées pendant 4 semaines. La sauvegarde quotidienne est incrémentale. Seules sont enregistrées les modifications de la journée. La sauvegarde hebdomadaire est totale. Toutes les données sont reprises le week-end.

5. Hébergement : Sécurité des Communications

5.1. Réseaux : Architecture générale

Le MiPih propose deux types de liens de communications pour accéder aux fonctionnalités des applications et services hébergés.

1. À travers le réseau privé étendu (WAN) des adhérents du MiPih qui permet l'interconnexion de sites et d'utilisateurs moyennant des réseaux privés virtuels (VPN) transportant le protocole IP. ADHERMIP est un réseau « clos » dédié aux usages du MiPih.
2. À travers le réseau Internet : Pour répondre aux exigences de sécurité imposées par son métier d'hébergeur, le MiPih a mis en place une architecture sécurisée permettant de garantir une très haute disponibilité des accès Internet.

   Le service est assuré par 2 opérateurs distincts : l'un à 30 Mbps symétriques et l'autre à 100 Mbps symétriques. Les accès sont redondants et fonctionnent en partage de charge. Leur débit est évolutif à la demande et n'entraîne pas d'interruption de service.

   Chaque liaison a été construite sur des parcours fibre optique. L'offre actuelle repose sur des accès RS3 (raccordement sécurisé de niveau 3), double connexion, parcours distincts, POP distincts sur chacun des sites géographiques.

   La continuité de service de l'accès internet est assurée par un accès opérateur sur le site de secours, ce dernier reprend l'activité du site principal en cas de défaillance simultanée des 2 accès principaux. Un mécanisme de peering BGP permet d'annoncer, de façon automatique, notre plan d'adresses IP public.

5.2. Interconnexion Toulouse – Amiens

Le MiPih dispose de 2 centres informatiques : un Datacenter principal situé à Toulouse et un Datacenter secondaire situé à Amiens.

Les deux sites sont raccordés par un réseau opérateur à très haut débit, le service est délivré sur un support fibre optique et le niveau de sécurisation est de type RS3 (Raccordement Sécurisé de niveau 3), soit une double connexion au niveau des bâtiments du MiPih, deux parcours fibres optiques totalement distincts et deux centres de rattachement distincts au réseau opérateur.

Un 3ième parcours souscrit auprès d'un second opérateur télécom permet d'élever le niveau de sécurisation en introduisant un 2ième opérateur sur les liaisons très haut débit.

Les liaisons entre les 2 Datacenters fonctionnent en mode nominal/secours et le protocole de routage OSPF permet de garantir un temps de bascule entre les différents parcours en dessous de 1 milliseconde.).

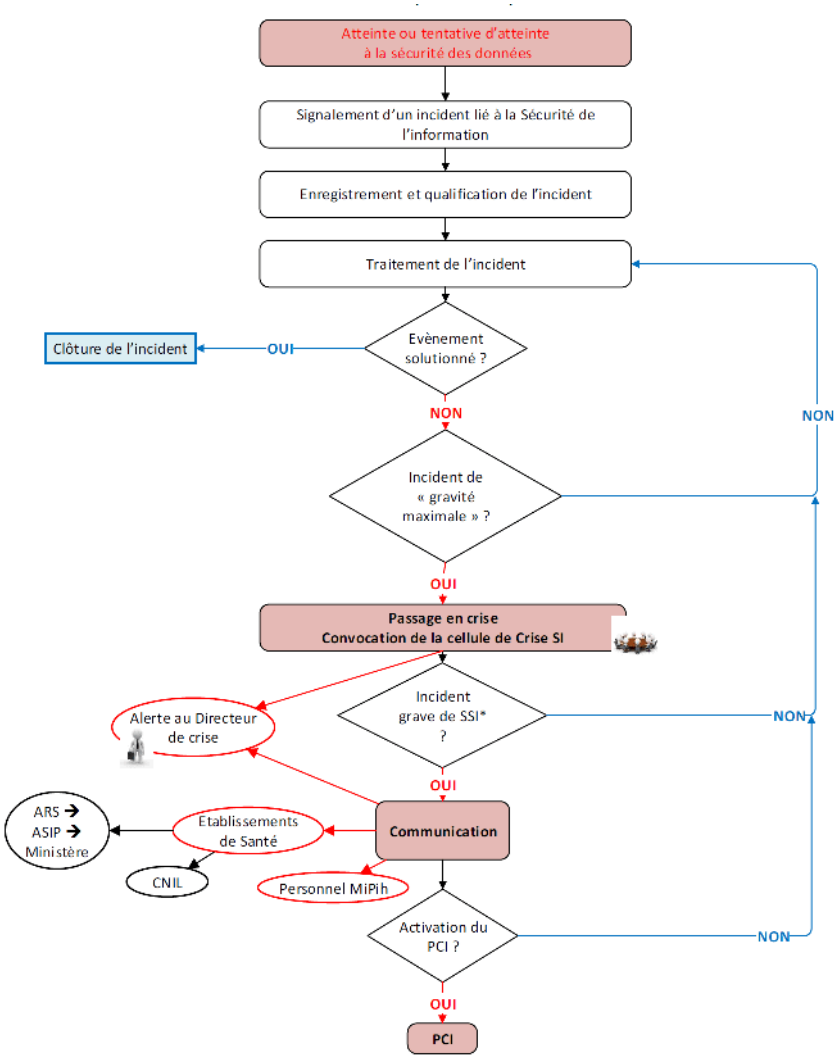
5.3. *Gestion des incidents*

5.3.1. *Incident portant atteinte à la sécuritédes informations*

Toute atteinte ou tentative d'atteinte à la sécurité des données, la disponibilité, l'intégrité, la confidentialité ou la preuve entraîne la création d'un incident de type « sécurité » affecté directement à un RSSI. L'analyse détaillée et le suivi des actions engagées sont enregistrés dans l'outil de gestion des incidents. Plus globalement les incidents y compris ceux affectant la sécurité des systèmes et des données hébergées sont traités comme décrit dans les chapitres suivants.

En outre, les établissements de santé sont responsables de l'application d'une politique de contrôle d'accès pour les utilisateurs des applications hébergées et l'accès aux données de santé.

Le schéma ci-dessous illustre les différentes étapes de la procédure :



5.3.2 *Traitement d'un incident de sécurité*

Les incidents enregistrés font l'objet d'un traitement spécifique en fonction de leur origine.

Les équipes techniques en charge du traitement de l'incident réalisent les actions nécessaires au rétablissement du service. Certaines demandes externes ou internes pouvant concerner la sécurité des SI sont soumis à la validation des RSSI et/ou des responsables de l'hébergement. Sans validation de leur part les demandes ne sont pas satisfaites.

Les RSSI et les responsables des services concernés par l'incident peuvent décider des actions complémentaires visant à :

- réduire les causes d'occurrence de l'incident :
- réduire la surface d'attaque,
- corriger les vulnérabilités,
- sensibiliser les acteurs,
- etc….

Un incident est clôturé que lorsque la solution proposée est validée par le demandeur

Addendum 3 - Spécificités liées à l'Hébergement de Données de Santé

Hébergeur certifié HDS

A la Date d'Entrée en Vigueur, le Service Hébergement des Données de Santé est confié au MiPih, Hébergeur Certifié HDS (N° 2018/80283.3).

Dans ce cadre, le MiPih garantit une sécurité accrue des Données de Santé traitées et le respect les lois et réglementations applicables en la matière.

Toute précision sur les conditions d'Hébergement des Données de Santé par le MiPih peut être communiquée sur demande écrite.

La Société se réserve le droit de sélectionner d'autres hébergeurs comme hébergeurs supplémentaires ou alternatifs à condition que ces hébergeurs soient Hébergeurs Certifiés HDS, et qu'un tel changement n'entraîne pas une diminution de la qualité du Service Hébergement.

Obligations de la Société

En sus de l'ensemble des engagements pris dans le cadre du Contrat et/ou qui lui sont applicables au titre des Lois et Réglementations sur la Protection des Données à Caractère Personnel, relatives au traitement des Données à Caractère Personnel et plus généralement relatives à la sécurité des Données, et outre le recours à un sous-traitant Hébergeur Certifié HDS, la Société reconnait que le traitement des Données de Santé et des Données Biométriques suppose une vigilance accrue et la mise en place de mesures techniques et organisationnelles adaptées aux risques.

De manière générale il est rappelé que la Société s'engage à :

- ne pas copier, extraire et/ou exploiter par quelque moyen que ce soit tout ou partie des Données, et ce incluant les Données de Santé qui pourraient être recueillies pour le compte du Client, étant précisé que les Données appartiennent au Client qui demeure le seul responsable du traitement ;
- garantir et maintenir la compétence, l'habilitation et la disponibilité de ses sous-traitants, collaborateurs, agents ou, qu'elle sensibilise aux enjeux relatives à l'Hébergement des Données de Santé. Les sous-traitants, collaborateurs, agents ou préposés restent placés sous son seul contrôle, sa seule autorité et sa seule direction.

Obligations du Client dans la relation avec la Société et son sous-traitant

Le Client s'engage quant à lui, outre ses obligations au titre du Contrat, à apporter sa totale collaboration à la Société et à ses sous-traitant, en particulier l'Hébergeur Certifié HDS désigné, s'agissant du traitement de ses Données de Santé pour permettre une réalisation conforme du Service Hébergement.

Dans ce cadre, le Client s'engage notamment à mettre à disposition de la Société toutes les informations qui lui sont nécessaires et à l'informer de toute spécificité ou changement de la législation ou de la règlementation concernant son métier et pouvant entraîner des conséquences particulières pour la Société.

S'agissant de l'administration de l'Environnement Client et des Données de Santé, le client s'engage à agir dans le respect :

- du Contrat ;
- des dispositions légales, réglementaires et déontologiques qui lui sont applicables. En particulier, le Client s'engage à respecter l'ensemble des obligations de la réglementation sur l'Hébergement des Données de Santé qui lui sont applicables et à mettre en œuvre les mesures techniques et organisationnelles associées. Le Client s'engage notamment, sans que cette liste ne soit exhaustive, à mettre en place un ensemble de procédures visant à :
    - recueillir le consentement des patients quant à l'enregistrement informatisé de leurs Données de Santé ;
    - recueillir le consentement des patients quant à l'Hébergement de leurs Données de Santé auprès d'un Hébergeur Certifié HDS ;
    - recueillir le consentement des patients quant à la transmission des Données de Santé les concernant à d'autres professionnels de santé, qu'ils soient internes ou externes à l'établissement ;
    - répondre aux demandes d'exercice de droits des patients ;
    - signaler les violation des Données à Caractère Personnel au sens des Lois et Réglementations sur la Protection des Données à Caractère Personnel et de manière générale tout faille de sécurité grave (altération des données, divulgation non autorisée des données, etc.).

- des mesures de sécurité spécifiques applicables au secteur de la santé et conforme à l'état de l'art et notamment aux documents applicables du corpus documentaire de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) ;
- des recommandations et conseils de la Société et de ses sous-traitants le cas échéant.

S'agissant de ses personnels et autre préposés (ci-après collectivement « les Agents »), le Client :

- veille à une mise à niveau régulière de leur formation ;

- sensibilise les agents accédant aux Données de Santé, à leurs obligations en matière de Données à Caractère Personnel, de confidentialité et plus généralement de respect du secret professionnel ;
- veille à ce que chaque Utilisateur respecte les règles de confidentialité de ses Données de Connexion. Le client s'engage à mettre en œuvre des procédures d'habilitations en interne et des systèmes d'authentification forte lorsque nécessaire ;
- définir les Profils Utilisateurs pouvant accéder aux Données de Santé hébergées.
- de manière générale, se porte fort des agissement de ses Agents.

Le descriptif de ces procédures, rédigées à l'initiative du Client, doit pouvoir être fourni à la Société sur simple demande. La Société ne peut être tenue responsable d'une non application de ces procédures. A ce titre, il est rappelé que le Client garantit la Société contre tout recours, plainte ou réclamation émanant d'une personne physique dont les Données seraient reproduites et hébergées par la Société.