

Conditions particulières Hébergement de Données de Santé (HDS)

Version du 1 septembre 2025

Table des matières

Table des matières.....	2
Article 1. – Objet.....	3
Article 2. – Définitions.....	3
Article 3. – Certification HDS.....	4
Article 4. – Localisations de l'hébergement.....	4
Article 5. – Accès à distance.....	4
Article 6. – Transferts de données de santé.....	5
Article 7. – Sous-traitance et prestataires.....	5
Article 8. – Communication.....	5
Article 9. – Partage de responsabilités.....	5
Article 10. – Description des prestations.....	6
Article 11. – Accès aux données de santé (DSCP).....	6
Article 12. – Évaluations de la performance.....	7
Article 13. – Droits des personnes concernées.....	8
Article 14. – Modifications ou évolutions techniques.....	9
Article 15. – Réversibilité des données.....	9
Article 16. – Régime financier applicable aux Contrats HDS.....	10
Annexe A. – Matrice RACI transversale.....	12
Annexe B. – Service d'hébergement sec.....	13
Annexe C. – Service d'hébergement d'équipement.....	14
Annexe D. – Service réseaux.....	15
Annexe E. – Service de serveur dédié.....	16
Annexe F. – Service de serveur virtuel.....	17
Annexe G. – Indicateurs de qualité et de performance.....	18

Article 1. – Objet

Les présentes conditions particulières, qui complètent les conditions générales de vente, les conditions particulières d'hébergement, les conditions particulières d'hébergement d'équipement, les conditions particulières des services réseaux, les conditions particulières de serveur dédié et/ou les conditions particulières serveur virtuel, ont pour objet de préciser les conditions particulières relatives à l'hébergement, par le client, de données de santé.

En cas de contrariété entre les conditions générales et/ou les conditions particulières susmentionnées avec les présentes conditions particulières, les clauses des conditions particulières Hébergement de Données de Santé (HDS) prévaudront pour le strict objet qui les concernent.

Article 2. – Définitions

Les définitions qui suivent sont fournies en complément des définitions contenues aux conditions générales de vente, aux conditions particulières mentionnées à l'article 1 :

Certification HDS : la certification définie et encadrée par l'article L.1111-8 du Code de la Santé Publique (CSP) et ses textes d'application qui a été obtenue par la Société CASTLE IT.

Données de santé : l'ensemble des données à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social et relatives à la santé physique et/ou mentale, passée, présente et/ou future, d'une personne physique.

Délégué à la protection des données (DPO) : le délégué à la protection des données est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Système de management de la sécurité de l'information (SMSI) : Un système de management de la sécurité de l'information est un ensemble de politiques visant la gestion de la sécurité de l'information.

Matrice RACI : Outil de répartition des responsabilités entre les Parties, permettant d'identifier pour chaque activité qui est :

- R (Responsible) : Réalisateur — Responsable de l'exécution;
- A (Accountable) : Approbateur — Garant de la réalisation (Porte la responsabilité finale);
- C (Consulted) : Consulté — Consulté préalablement;
- I (Informed) : Informé — Informé a posteriori.

La matrice RACI vise à assurer une compréhension commune des rôles et obligations de la société CASTLE IT et du Client dans le cadre de la prestation d'hébergement de données de santé.

Incident : Désigne tout événement affectant ou susceptible d'affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité des services fournis, et nécessitant une intervention de CASTLE IT.

Ticket : Désigne la demande ou déclaration d'incident enregistrée par le Client via l'outil de gestion de ticket mis à disposition par CASTLE IT.

Article 3. – Certification HDS

Certificat HDS – La société CASTLE IT a, conformément à L.1111-8 du Code de la Santé Publique (CSP) et ses textes d'application, obtenu, le 30/10/2025, la certification hébergeur de données de santé. Une copie dudit certificat est remise au client à la signature du contrat. Elle est par ailleurs accessible en ligne : www.castle-it.fr/cgv

Cette certification a une durée de validité allant jusqu'au 29/10/2028.

La Société CASTLE IT s'engage à maintenir cette certification et/ou toute autre autorisation prévue par la loi française pour toute la durée du contrat la liant au client.

En cas de suspension ou retrait du certificat, la société CASTLE IT s'engage à en informer sans délai le client par tous moyens.

Le retrait définitif de la certification emporte la résiliation de plein droit du contrat.

En cas de suspension ou retrait temporaire, le client aura la faculté de résilier le contrat en notifiant cette demande par courrier recommandé avec accusé de réception. La date de la résiliation sera celle de réception du courrier.

Périmètre – La certification obtenue porte sur le périmètre suivant :

1. La mise à disposition et le 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 ;
2. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;
3. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
4. La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;

Article 4. – Localisations de l'hébergement

L'ensemble des données sont hébergées et stockées sur le(s) site(s) de la Société CASTLE IT et, en tout état de cause, ne le seront qu'en France.

La documentation, les interfaces utilisateur ainsi que le support sont rédigées à minima, en langue française.

Article 5. – Accès à distance

L'accès à distance aux données de santé ne pourra être réalisé que depuis un pays membre de l'Espace Économique Européen.

Article 6. – Transferts de données de santé

Aucun transfert des données de santé à caractère personnel vers un pays tiers à l'Espace Économique Européen ne sera réalisé.

Article 7. – Sous-traitance et prestataires

La société CASTLE IT ne sous-traite aucune des prestations d'hébergement vendues.

Pour l'hypothèse où la Société CASTLE IT devrait faire appel à des prestataires techniques extérieurs, elle en tiendra informé le client et garantit un niveau de protection équivalent à celui auquel elle est tenue.

En cas de recours à un sous-traitant, la société CASTLE IT transmettra au client le contrat HDS ou certificat en vigueur du prestataire concerné. CASTLE IT s'assurera en tout temps du maintien de la certification HDS du sous-traitant et des mesures de sécurité suffisantes conformes à la réglementation en vigueur. En cas de suspension, retrait ou non-renouvellement de la certification dudit sous-traitant, la société CASTLE IT en informera sans délai le Client et proposera une solution de remplacement conforme aux exigences HDS.

Article 8. – Communication

Le Client communiquera à la signature du contrat une fiche de renseignement "Renseignement contact HDS" qui contient les coordonnées du référent contractuel à contacter pour le traitement des incidents ayant un impact sur les données de santé. Ce référent doit notamment être en mesure de désigner à CASTLE IT un professionnel de santé habilité à accéder aux données de santé lorsque cela est nécessaire.

Le client s'engage à maintenir à jour les coordonnées de ce référent contractuel en les notifiant, en cas de modification(s), sans délai à la CASTLE IT.

Les coordonnées de ce référent pourront être transmises par CASTLE IT aux autorités compétentes qui en feront la demande, notamment en cas de suspension ou retrait de la certification mentionnée à l'article 3.

Article 9. – Partage de responsabilités

La société CASTLE IT est tenue d'une obligation générale de moyens et s'engage à ce titre à fournir le service d'hébergement conformément aux règles de l'art de sa profession. Elle s'engage dans ce cadre à garantir la disponibilité, l'intégrité, la confidentialité, l'auditabilité et la traçabilité des données hébergées. CASTLE IT est seule responsable des moyens et méthodes qu'elle met en œuvre dans le cadre de la fourniture du service d'hébergement, lesquels sont détaillés dans les conditions générales de vente et les conditions particulières mentionnées à l'article 1. Le client déclare en avoir pris connaissance et les accepter sans réserve.

CASTLE IT assure une surveillance constante pour relever tout incident et/ou défaillance impactant les services d'hébergement.

Dans l'hypothèse d'une défaillance du service, CASTLE IT s'engage à en informer le client dès l'instant où cette défaillance a un impact éventuel ou avéré sur l'hébergement de ses données de santé. CASTLE IT s'engage à tout mettre en œuvre pour y remédier dans les meilleurs délais.

Pour l'hypothèse de toute attaque et/ou intrusion qu'elle constaterait, la société CASTLE IT fera ses meilleurs efforts pour les faire cesser, en réduire l'impact sur la disponibilité du service d'hébergement et la confidentialité des données. Elle transmettra au client l'ensemble des éléments de preuve collectés permettant d'identifier son (ses) auteur(s).

Le client s'engage à informer sans délai CASTLE IT de toute défaillance/incident qu'il aurait identifié.

Le contact professionnel de santé du client sera associé à l'ensemble de processus de gestion des incidents en sa qualité de garant de la confidentialité des données de santé hébergées.

En tout état de cause la société CASTLE IT ne pourra pas être retenue pour les cas suivants :

- Pertes ou altérations des données en l'absence de sauvegardes réalisées périodiquement par le client qui en est seul responsable ;
- Inaccessibilité à la solution d'hébergement si l'origine de cette inaccessibilité résulte des équipements relevant de la maîtrise du client ;
- Intrusions ou utilisations non-autorisées ou illicites des identifiants et mots de passe du client sauf s'il est démontré par le client qu'elles résultent d'une défaillance de la société CASTLE IT dans la sécurisation de la prestation d'hébergement souscrite ;
- Préjudices subis par le client ou des tiers en raison du contenu hébergé dont le client a la seule maîtrise et gestion.

Est annexée ci-après (Annexe A) une matrice RACI transversale. Cette matrice définit, pour les activités transversales essentielles à l'hébergement de données de santé, les responsabilités respectives de CASTLE IT et du Client.

Cette matrice complète le présent article. Elle pourra être mise à jour par avenant contractuel en cas d'évolution de la réglementation, de la certification HDS ou des services fournis.

Article 10. – Description des prestations

Pour toutes prestations, telles que précisées en annexes B, C, D, E et F ci-après reproduites, la Société CASTLE IT s'engage à prendre toutes mesures techniques et/ou organisationnelles nécessaires pour garantir la protection des DSCP hébergées, notamment leur disponibilité, leur intégrité, leur confidentialité et leur auditabilité.

Article 11. – Accès aux données de santé (DSCP)

La société CASTLE IT n'a aucun accès aux données de santé du client. Les données de santé hébergées ne pourront être traitées par CASTLE IT que dans la finalité de l'exécution de l'activité d'hébergement souscrite. Tout autre usage des données de santé par CASTLE IT est interdit.

En dehors des mesures de sécurité mises en œuvre par la société CASTLE IT pour sécuriser l'accès aux hébergements souscrits (définis dans les conditions générales et particulières mentionnées à l'article 1) le client est seul responsable de l'accès à ses données de santé.

Le client s'engage en conséquence à mettre en œuvre les moyens de contrôle d'accès et de gestion des identités adaptés pour les utilisateurs qui utilisent les prestations d'hébergement souscrites.

Le chiffrement des données au repos (disques, supports de sauvegarde) et des flux réseaux relève de la seule responsabilité du Client. La société CASTLE IT garantit la compatibilité technique de ses infrastructures avec ces mécanismes de chiffrement, mais n'en assure pas la mise en œuvre.

L'accès aux prestations est assuré par les clés d'accès aux services (ensemble des identifiants permettant au client de pouvoir consommer et piloter les prestations). Les clés sont dédiées à un compte précis. Le client s'engage à ne pas les partager.

Le client s'engage à réaliser la sauvegarde des données de santé qu'il héberge et en est seul responsable. L'attention du client est attirée sur la nécessité de réaliser des sauvegardes régulières eu égard aux risques existant en son absence (perte et/ou dommages affectant les données).

La société CASTLE IT ne propose pas de prestation de sauvegarde dans le cadre de la certification HDS.

La société CASTLE IT pourra réaliser des contrôles portant sur le respect des conditions susmentionnées.

Article 12. – Évaluations de la performance

Le client aura la possibilité de réaliser ou mandater, au maximum une fois par an, des audits de sécurité technique sur ses seules ressources spécifiques. Le client doit en informer au préalable la société CASTLE IT avec un délai de prévenance d'au moins trente jours. La date et l'horaire de l'audit seront fixés d'un commun accord sous les meilleurs délais. La société CASTLE IT se réserve la faculté de refuser le prestataire désigné en cas de risque de conflits d'intérêts ou de concurrence. Les frais inhérents à cet audit seront exclusivement à la charge du client. Les ressources engagées par CASTLE IT pour les besoins de l'audit, notamment l'assistance du client lors de l'audit, seront facturées au client.

Toutes les informations entrant dans le cadre de l'audit, y compris les informations intégrées aux conclusions de l'audit, seront soumises à une stricte confidentialité ; Le client devra en conséquence justifier auprès de CASTLE IT que l'auditeur par lui désigné est soumis à une obligation de confidentialité.

Le client remettra gratuitement à la société CASTLE IT le rapport d'audit. Dans l'hypothèse où des écarts à la réglementation applicable et à la certification HDS seraient constatés, les parties s'engagent à échanger et collaborer de bonne foi pour la mise en œuvre des mesures nécessaires.

CASTLE IT se réserve la faculté d'exclure certains éléments du périmètre de l'audit, notamment les éléments mutualisés.

CASTLE IT s'engage à fournir sur demande écrite du client, la synthèse managériale d'un rapport d'audit réalisé par un auditeur extérieur et indépendant datant de moins de trois ans, portant sur les parties d'audit qu'elle aurait exclues de l'audit réalisé à l'initiative du client (notamment les éléments mutualisés).

Sur demande écrite le client aura la possibilité de consulter les traces d'accès aux données de santé portées par des ressources spécifiques ou aux dites ressources par le personnel de CASTLE IT.

Sur demande écrite réalisée par courrier recommandé avec accusé de réception, le client aura la possibilité de consulter sur le site de la société CASTLE IT, au jour et à l'heure convenus d'un commun accord, le dernier rapport d'audit de la certification HDS. La copie de tout ou partie de ce rapport est interdite. Le contenu du rapport d'audit est soumis à une stricte confidentialité.

CASTLE IT s'engage à réaliser chaque année des audits internes permettant de déterminer :

- Si le SMSI est conforme aux exigences de la certification HDS et est efficacement mis en œuvre et maintenu.
- Les traces des accès, par les personnes opérant pour le compte du client, aux données de santé ou aux systèmes utilisés pour leur traitement. La traçabilité des données relève de la seule responsabilité du client.

Outre les audits mentionnés ci-dessus, le niveau des services sera vérifiable selon les indicateurs de performance et de qualité détaillés en Annexe G

Article 13. – Droits des personnes concernées

Le client garantit le respect de la législation relative aux droits des personnes dont les données de santé sont collectées et hébergées. En particulier, le client garantit à CASTLE IT qu'il a informé les personnes concernées de ce que leurs données de santé personnelles seront stockées sur les serveurs de la société CASTLE IT et qu'il a, le cas échéant, recueilli leur consentement à cet effet.

Le client est seul responsable de l'exercice des droits des personnes sur les données personnelles de santé qui les concernent.

La société CASTLE IT s'engage à collaborer avec le client pour lui que ce dernier puisse s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, droit de rectification, droit d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données personnelles, droit de pas faire l'objet d'une décision individuelle automatisée (y compris profilage).

Si les personnes concernées devaient formuler une demande directement auprès de la société CASTLE IT (dpo@castle-it.fr), cette dernière les adressera sans délai, par voie électronique, au client afin qu'il puisse répondre à leurs demandes dans le délai légal d'un mois. La société CASTLE IT ne répondra pas directement à la personne ayant formulé une demande.

Dans l'hypothèse d'une violation des données à caractère personnel portée à sa connaissance, la société CASTLE IT s'engage à en informer sans délai le client et à coopérer avec ce dernier pour prendre toute mesure utile pour remédier à la situation.

Des audits seront menés par le délégué à la protection des données pour s'assurer du respect de la législation en vigueur.

Article 14. – Modifications ou évolutions techniques

Le client reconnaît et accepte que CASTLE IT pourrait être amenée à modifier les services ou mettre en place de nouveaux services afin d'apporter les évolutions techniques nécessaires à la réalisation de ses services ou lorsque ces évolutions ou modifications sont imposées par la cadre légal applicable, en particulier celui lié à l'hébergement des données de santé.

L'introduction de nouveaux services ou modification ou maintenance des services existants font l'objet d'une communication au client au moins une semaine avant leur mise en service sauf urgence impérieuse.

L'accord préalable du client sera nécessaire dans le cas où les modifications ou évolutions ne respectent pas les niveaux de services tels que convenus initialement, notamment eu égard à la disponibilité, l'intégrité, la confidentialité, l'audibilité des données de santé hébergées ou encore les procédures et garanties dues en cas de défaillance du service.

Dans l'hypothèse où les évolutions imposées entraîneraient un changement de circonstances imprévisibles au moment de la conclusion du contrat, la partie qui n'a pas accepté d'assumer le risque d'exécution excessivement onéreux pourra demander une renégociation du contrat.

Article 15. – Réversibilité des données

Au terme du contrat d'hébergement de données de santé, quelle qu'en soit la cause, CASTLE IT assurera la réversibilité des données confiées au titre de la prestation confiée et restituera la totalité des DSCP dans les conditions suivantes :

La réversibilité consiste à permettre au client de récupérer toutes ses données hébergées.

Lors de la résiliation du contrat, quelle qu'en soit la cause ou l'initiateur, le client aura accès pour une durée de cinq jours aux données stockées afin d'en assurer lui-même, sous sa seule responsabilité, la réversibilité.

Au plus tard à l'issue de ce délai de 10 jours calendaires, à compter de la date de résiliation effective du contrat, le client devra faire parvenir à la société CASTLE IT un procès-verbal "récupération des données".

À compter de la réception de ce procès-verbal "récupération des données" la société CASTLE IT mettra fin à l'accès nécessaire à la récupération des données, effacera, hors hypothèse d'une prestation « hébergement », « hébergement d'équipement » ou « réseaux », toutes les données du client et n'en gardera aucune trace.

Toutes les données seront effacées définitivement au plus tard sept jours après la réception du procès-verbal "récupération des données", le tout conformément à la réglementation en vigueur.

Si, à l'issue d'un délai 6 jours après réception du courrier notifiant la résiliation, le client n'a pas retourné le procès-verbal "récupération des données" signé, après mise en demeure par lettre recommandée avec accusé de réception d'émettre ledit procès-verbal "récupération des données" restée infructueuse pendant

sept jours calendaires, la société CASTLE IT pourra facturer l'immobilisation des espaces de stockage sur lesquels les données sont encore présentes pendant cinq mois. Au-delà de ce délai la société CASTLE IT sera fondée à supprimer définitivement les données stockées, ce que le client reconnaît et accepte.

Dans l'hypothèse d'une prestation « hébergement », « hébergement d'équipement » ou « réseaux », le client sera facturé pour une durée de 5 mois maximum selon les conditions du contrat « hébergement », « hébergement d'équipement » ou « réseaux » souscrit(s). A l'issue de ce délai la Société CASTLE IT sera fondée à réaliser ou faire réaliser, aux seuls frais du client et sous la seule responsabilité de ce dernier, l'enlèvement et la destruction de l'ensemble des matériels du client.

Un certificat d'effacement/destruction des données de santé, conforme à la réglementation en vigueur, sera remis au client par CASTLE IT.

La destruction du disque dur sera facturée au client à une somme qui sera calculée de la manière suivante : prix (TTC) de la prestation de destruction du (des) disque(s) dur(s) par un tiers habilité, augmentée d'une somme forfaitaire de 5% de ce prix.

Le client a la possibilité de demander, dans un délai maximal de cinq jours suivant réception de la notification de la résiliation du contrat, à ce que la Société CASTLE IT réalise les prestations complémentaires suivantes, qui feront l'objet d'un bon de commande spécifique :

- Pour la prestation « serveur dédié » : remise des disques contenant les DSCP dans un délai maximum de 48 heures suivant décommissionnement du serveur. Le client devra désigner avec précision la personne habilitée à venir chercher sur le site de la société CASTLE IT lesdits disques. Un procès-verbal « récupération des données » sera signé par le client, ou la personne habilitée à réceptionner les disques, au moment de la remise des disques. A compter de cette remise le client sera seul responsable des DSCP remises qu'il s'agisse notamment de leur intégrité, confidentialité et destruction. La récupération d'un disque physique est facturée au tarif de dix (10) fois le prix récurrent mensuel du disque concerné. Toutefois, pour les contrats d'une durée supérieure à soixante (60) mois, ce tarif est remplacé par un montant forfaitaire de 50 € HT par disque.
- Pour la prestation « serveur virtuel » : remise d'une image du disque virtuel au format RAW ou QCOW2. Cette remise sera réalisée via l'envoi du fichier sur un SFTP sécurisé mis à disposition par le client. Un procès-verbal « récupération des données » sera signé par le client, ou la personne habilitée à réceptionner ce fichier, au moment de la remise de ce fichier. A compter de cette remise le client sera seul responsable des DSCP remises qu'il s'agisse notamment de leur intégrité et confidentialité. La fourniture d'une image disque virtuel (au format RAW ou QCOW2, remise via SFTP sécurisé) est facturée à 50 € HT par disque virtuel.

Article 16. – Régime financier applicable aux Contrats HDS

Dans l'hypothèse où un Service est qualifié "HDS" à la suite d'une notification écrite émise par le Client et dûment acceptée par Castle IT, ledit Service est soumis au régime financier dérogatoire défini au présent article.

À ce titre, il est expressément convenu entre les Parties que chaque Service qualifié HDS donnera lieu à l'application d'une majoration tarifaire spécifique, égale à dix pour cent (10 %) du montant récurrent mensuel hors taxes afférent au Service concerné. Cette majoration est facturée mensuellement, concomitamment à la facturation ordinaire des Produits et Service souscrits.

Nonobstant la règle proportionnelle ci-dessus, il est stipulé que le montant cumulé des majorations afférentes aux Service qualifié HDS pour une même période de facturation ne saurait être inférieur à un montant minimum forfaitaire de cent cinquante euros (150 €) hors taxes.

La facturation d'un service en tant que "Service qualifié HDS" demeure applicable jusqu'à réception et prise d'effet, par Castle IT, d'une demande écrite de résiliation dudit service "HDS" émise par le Client. Cette prise d'effet interviendra à la prochaine échéance de facturation mensuelle, sauf disposition contraire convenue par écrit entre les Parties.



Annexe A. – Matrice RACI transversale

Article 1 – Objet

La présente annexe a pour objet de définir, de manière exhaustive et contraignante, la répartition des rôles et responsabilités entre CASTLE IT et le Client, dans le cadre de la prestation d'hébergement de données de santé (HDS) régie par les présentes conditions particulières.

Elle précise, pour chaque activité essentielle liée à la sécurité, à la conformité réglementaire et à la gestion des données de santé, les parties responsables de leur exécution, de leur approbation, de leur consultation ou de leur information, conformément à la méthodologie RACI (Responsible, Accountable, Consulted, Informed).

Cette matrice s'applique en complément des présentes conditions particulières, ainsi qu'aux obligations légales et réglementaires en vigueur, notamment celles issues du Règlement Général sur la Protection des Données (RGPD) et du référentiel HDS v2.

Article 2 – Répartition des responsabilités

La répartition des responsabilités entre CASTLE IT et le Client est définie conformément à la matrice RACI :

Activité	CASTLE IT	Client
Maintien de la certification HDS	R/A	I
Information en cas de retrait/suspension de certification	R	I
Notification d'incident de sécurité	R	A
Respect du RGPD	C	R/A
Audits HDS	R	C
Réversibilité / Effacement / Destruction des données	R	A
Sauvegardes régulières des données	I	R/A
Sécurité physique et environnementale	R/A	I

Légende : R (Réalisateur), A (Approbateur), C (Consulté), I (Informé).

Annexe B. – Service d'hébergement sec

Article 1 – Description du service

Le service d'hébergement sec met à disposition des clients un espace physique sécurisé au sein du centre de données (baies, armoires ou salles privatives) destiné à accueillir leurs propres équipements informatiques. Il comprend l'accès à l'infrastructure essentielle du site : alimentation électrique redondée, climatisation et régulation de la température ainsi qu'une sécurité physique renforcée (contrôle d'accès, vidéosurveillance, détection incendie). Ce service permet aux clients de garder la maîtrise totale de leurs équipements tout en bénéficiant de la fiabilité et de la résilience d'un environnement en centre de données.

Article 2 – Répartition des responsabilités

La répartition des responsabilités entre CASTLE IT et le Client est définie conformément à la matrice RACI :

Activité	CASTLE IT	Client
Maintenance infrastructure (climatisation, électricité)	R/A	I
Installation et maintenance des équipements IT	I	R/A
Sauvegarde des données	I	R/A
Surveillance des conditions environnementales	R/A	I
Accès aux équipements	I	R/A

Légende : R (Réalisateur), A (Approbateur), C (Consulté), I (Informé).

Article 3 – Indicateur de disponibilité

Article 3.1 – Définition

Le taux de disponibilité correspond au pourcentage de temps, sur une période mensuelle, durant lequel l'alimentation électrique, la température et l'humidité relative fournies par CASTLE IT pour l'hébergement sont pleinement opérationnelles, hors périodes de maintenance planifiée notifiées conformément au présent contrat.

Article 3.2 – Objectif

CASTLE IT garantit une disponibilité minimale de 99,9 % par mois.

(Le mode de mesure, la périodicité et l'application des pénalités sont définis à l'Annexe G.)

Annexe C. – Service d'hébergement d'équipement

Article 1 – Description du service

Le service d'hébergement d'équipements consiste à mettre à disposition des clients un espace physique sécurisé (baies, armoires ou salles privatives) pour l'installation de leurs serveurs et infrastructures IT. Ce service inclut une alimentation électrique redondée et garantie, un système de climatisation et de contrôle thermique, ainsi que des dispositifs de sécurité physique avancés (contrôle d'accès, vidéosurveillance, détection incendie). Les clients bénéficient également d'une connectivité réseau redondée, assurant la disponibilité et l'accessibilité de leurs systèmes dans un environnement hautement fiable et conforme aux standards du secteur.

Article 2 – Répartition des responsabilités

La répartition des responsabilités entre CASTLE IT et le Client est définie conformément à la matrice RACI :

Activité	CASTLE IT	Client
Fourniture d'alimentation et réseau redondant	R/A	I
Installation, configuration, administration des serveurs	I	R/A
Mise en œuvre du chiffrement (données/flux)	I	R/A
Sauvegardes	I	R/A
Supervision disponibilité	R	A

Légende : R (Réalisateur), A (Approbateur), C (Consulté), I (Informé).

Article 3 – Indicateur de disponibilité

Article 3.1 – Définition

Le taux de disponibilité correspond au pourcentage de temps, sur une période mensuelle, durant lequel l'alimentation électrique et la connectivité réseau fournie par CASTLE IT pour l'hébergement d'équipement sont pleinement opérationnelles, hors périodes de maintenance planifiée notifiées conformément au présent contrat.

Article 3.2 – Objectif

CASTLE IT garantit une disponibilité minimale de 99,9 % par mois de l'alimentation électrique et de la connectivité réseau.

(Le mode de mesure, la périodicité et l'application des pénalités sont définis à l'Annexe G.)

Annexe D. – Service réseaux

Article 1 – Description du service

Les services réseaux comprennent la mise à disposition de routeur virtuel, d'une connectivité réseau sécurisée, l'attribution d'adresses IP publiques, la configuration de règles de filtrage (firewall de niveau 3), la gestion de la translation d'adresses (NAT entrant et sortant), ainsi que la mise en place de tunnels VPN (IPsec/SSL) pour garantir un accès distant protégé.

Article 2 – Répartition des responsabilités

La répartition des responsabilités entre CASTLE IT et le Client est définie conformément à la matrice RACI :

Activité	CASTLE IT	Client
Mise en place et supervision réseau	R/A	I
Isolement entre clients	R/A	I
Gestion des adresses IP / NAT / firewall	R	A
Mise en place et gestion des VPN IPsec	R	R/A
Mise en place et gestion des VPN SSL	I	R/A
Chiffrement des flux applicatifs (TLS, etc.)	I	R/A
Gestion des incidents de sécurité réseau	R	A
Documentation et reporting réseau	R	I

Légende : R (Réalisateur), A (Approbateur), C (Consulté), I (Informé).

Article 3 – Indicateur de disponibilité

Article 3.1 – Définition

Le taux de disponibilité correspond au pourcentage de temps, sur une période mensuelle, durant lequel les équipements et services réseaux fournis par CASTLE IT (backbone, pare-feu, routeurs, commutateurs) sont pleinement opérationnels, hors périodes de maintenance planifiée notifiées conformément au présent contrat.

Article 3.2 – Objectif

CASTLE IT garantit une disponibilité mensuelle minimale de 99,9 % du service réseaux.

(Le mode de mesure, la périodicité et l'application des pénalités sont définis à l'Annexe G.)

Annexe E. – Service de serveur dédié

Article 1 – Description du service

Le service de location de serveurs physiques dédiés permet aux clients de disposer de machines entièrement réservées à leurs usages, hébergées dans un datacenter sécurisé. Ces serveurs offrent des performances garanties, une haute disponibilité et une flexibilité dans le choix des configurations (processeurs, mémoire, stockage). Le client conserve un contrôle total sur son environnement (système d'exploitation, applications, paramètres de sécurité), tout en bénéficiant des avantages de l'infrastructure du datacenter : alimentation redondée, climatisation, supervision, et sécurité physique renforcée.

Article 2 – Répartition des responsabilités

La répartition des responsabilités entre CASTLE IT et le Client est définie conformément à la matrice RACI :

Activité	CASTLE IT	Client
Fourniture et maintenance matérielle	R/A	I
Accès logique (système, applications)	I	R/A
Administration du serveur (OS, applications, comptes utilisateurs)	I	R/A
Mise en place sauvegardes	I	R/A
Mise en place du chiffrement (disques, flux)	I	R/A
Supervision matérielle	I	R/A
Gestion des incidents sécurité	R	A

Légende : R (Réalisateur), A (Approbateur), C (Consulté), I (Informé).

Article 3 – Indicateur de disponibilité

Article 3.1 – Définition

Le taux de disponibilité correspond au pourcentage de temps, sur une période mensuelle, durant lequel le matériel du serveur dédié mis à disposition du Client est pleinement opérationnel, à l'exclusion des disques de stockage internes dont la surveillance est sous la responsabilité du Client.

Article 3.2 – Objectif

CASTLE IT garantit une disponibilité mensuelle minimale de 99,9 % du matériel du serveur dédié, hors disques de stockage.

(Le mode de mesure, la périodicité et l'application des pénalités sont définis à l'Annexe G.)

Annexe F. – Service de serveur virtuel

Article 1 – Description du service

Le service de location de serveurs virtuels offre aux clients un environnement informatique flexible et évolutif, reposant sur une infrastructure de virtualisation hébergée dans un datacenter sécurisé. Chaque serveur virtuel dispose de ressources dédiées (processeur, mémoire, stockage) et peut être personnalisé en fonction des besoins. Ce service permet de bénéficier rapidement de capacités de calcul performantes sans investissement matériel, tout en garantissant haute disponibilité, redondance, supervision continue et sécurité renforcée.

Article 2 – Répartition des responsabilités

La répartition des responsabilités entre CASTLE IT et le Client est définie conformément à la matrice RACI :

Activité	CASTLE IT	Client
Fourniture et maintenance plateforme de virtualisation	R/A	I
Isolement entre clients	R/A	I
Administration du serveur (OS, applications, comptes utilisateurs)	I	R/A
Mise en place sauvegardes	I	R/A
Mise en place du chiffrement (disques, flux)	I	R/A
Supervision disponibilité	R	I
Gestion des incidents sécurité	R	A

Légende : R (Réalisateur), A (Approbateur), C (Consulté), I (Informé).

Article 3 – Indicateur de disponibilité

Article 3.1 – Définition

Le taux de disponibilité correspond au pourcentage de temps, sur une période mensuelle, durant lequel l'infrastructure de virtualisation permettant l'exécution du serveur virtuel du Client est pleinement opérationnelle, hors périodes de maintenance planifiée.

Article 3.2 – Objectif

CASTLE IT garantit une disponibilité mensuelle minimale de 99,9 % pour les serveurs virtuels.

(Le mode de mesure, la périodicité et l'application des pénalités sont définis à l'Annexe G.)

Annexe G. – Indicateurs de qualité et de performance

Article 1 – Objet

La présente annexe définit les indicateurs de qualité et de performance applicables aux prestations d'hébergement de données de santé fournies par CASTLE IT.

Ces indicateurs sont suivis selon la périodicité indiquée et pourront être consultés par le Client sur simple demande écrite.

Article 2 – Indicateurs

Article 2.1 – Taux de disponibilité

- **Définition** : Le taux de disponibilité correspond au pourcentage de temps, sur une période mensuelle, durant lequel le service concerné est pleinement opérationnel, hors périodes de maintenance planifiée notifiées conformément au présent contrat.
La définition détaillée de la disponibilité pour chaque service figure dans les annexes correspondantes (Annexes B à F).
- **Objectif** : L'objectif de disponibilité contractuel varie en fonction du service fourni et est précisé dans les annexes correspondantes (Annexes B à F).
- **Mesure** : La disponibilité est mesurée par les outils de supervision de CASTLE IT (infrastructure, réseau, hyperviseurs, serveurs physiques) et par l'analyse des journaux techniques. Toute interruption de service supérieure à une (1) minute est comptabilisée.
- **Périodicité** : Le calcul du taux de disponibilité est effectué mensuellement. Un rapport de disponibilité est mis à disposition du Client sur l'interface client.
- **Pénalités** : Applicables (Voir Article 3 – Pénalités applicables).

Article 2.2 – Sécurité physique

- **Définition** : La sécurité physique désigne l'ensemble des mesures de contrôle mises en œuvre par CASTLE IT pour assurer la protection des infrastructures du centre de données, incluant notamment les dispositifs de contrôle d'accès (badges, biométrie), la vidéosurveillance, la détection incendie et la détection d'intrusion.
- **Objectif** : CASTLE IT garantit que l'accès aux zones hébergeant les équipements du Client est strictement limité aux personnes autorisées, et que 100 % des accès physiques sont soumis à contrôle et journalisation.
- **Mesure** : La conformité est mesurée par la tenue et l'examen des journaux d'accès physiques, des enregistrements de vidéosurveillance et des rapports d'intervention. Tout accès est tracé, daté et associé à une identité autorisée.
- **Périodicité** : La revue des journaux d'accès et des dispositifs de sécurité physique est réalisée mensuellement, et les preuves de conformité sont conservées pour une durée minimale de trois (3) ans.
- **Pénalités** : Non-applicables.

Article 2.3 – Traçabilité des interventions

- **Définition** : La traçabilité des interventions correspond à l'enregistrement systématique, dans l'outil de gestion des tickets de CASTLE IT, de toute opération réalisée sur les infrastructures hébergeant les équipements du Client, incluant l'installation, la maintenance, le contrôle ou le retrait de matériel.
- **Objectif** : CASTLE IT garantit que 100 % des interventions sont consignées dans l'outil de gestion des tickets, précisant la date et l'heure de l'intervention, l'identité de l'intervenant, la nature de l'opération, ainsi que, le cas échéant, l'autorisation préalable donnée par le Client.
- **Mesure** : Le respect de cet objectif est mesuré par l'examen des tickets enregistrés dans l'outil de gestion des tickets.
- **Périodicité** : La saisie des interventions dans l'outil de gestion des tickets est effectuée à chaque opération. L'historique des tickets est conservé pour une durée minimale de trois (3) ans.
- **Pénalités** : Non-applicables.

Article 2.4 – Délai de prise en charge des incidents

- **Définition** : Le délai de prise en charge des incidents correspond au temps écoulé entre l'ouverture d'un ticket incident par le Client et sa première prise en charge effective par CASTLE IT.
- **Objectif** : CASTLE IT garantit une prise en charge dans un délai inférieur à quatre (4) heures ouvrées, dans la plage horaire de 09h00 à 17h30, du lundi au vendredi, hors jours fériés.
- **Mesure** : Le respect de cet objectif est mesuré par l'examen des tickets enregistrés dans l'outil de gestion des tickets, permettant de comparer l'heure d'ouverture du ticket avec l'heure de sa première prise en charge.
- **Périodicité** : La mesure est effectuée sur une base mensuelle.
- **Pénalités** : Non-applicables.

Article 2.5 – Rapports d'audit interne et externe

- **Définition** : Les rapports d'audit interne et externe correspondent aux vérifications documentées de conformité aux référentiels applicables, notamment la norme ISO 27001, le référentiel HDS v2 et le RGPD, réalisées soit par CASTLE IT (audit interne), soit par un tiers indépendant (audit externe).
- **Objectif** : CASTLE IT garantit la réalisation d'au moins un (1) audit interne par an, ainsi que la mise à disposition du Client, sur demande, d'un rapport ou d'une synthèse d'audit externe datant de moins de trois (3) ans.
- **Mesure** : Le respect de cet objectif est mesuré par la production des rapports d'audit interne et externe et par la mise à disposition des conclusions correspondantes.
- **Périodicité** : Les audits internes sont réalisés au moins une (1) fois par an et les audits externes au moins tous les trois (3) ans.
- **Pénalités** : Non-applicables.

Article 2.6 – Communication des incidents de sécurité

- **Définition** : La communication des incidents de sécurité correspond au délai maximal dans lequel CASTLE IT s'engage à informer le Client de la survenance d'un incident affectant la confidentialité, l'intégrité ou la disponibilité des données ou des services.
- **Objectif** : CASTLE IT garantit que tout incident de sécurité est notifié au Client dans un délai maximal de deux (2) heures suivant sa détection par ses systèmes de supervision ou par son équipe de sécurité.
- **Mesure** : Le respect de cet objectif est mesuré par la l'outil de gestion de ticket et par les journaux de supervision et d'alerte.
- **Périodicité** : Notification immédiate en cas d'incident ; consolidation dans un rapport mensuel.
- **Pénalités** : Non-applicables.

Article 3 – Pénalités applicables

Article 3.1 – Principe

En cas de non-respect des engagements de disponibilité définis à l'article 2.1, le Client peut bénéficier d'une indemnité financière dite « Pénalité de Service », imputée sur la facture mensuelle suivante.

Article 3.2 – Barème

- Pour un service garanti à 100 % de disponibilité mensuelle :
une pénalité de dix pour cent (10 %) du montant de l'abonnement mensuel par tranche de vingt (20) minutes d'indisponibilité, dans la limite de cent pour cent (100 %) du montant de l'abonnement mensuel.
- Pour un service garanti à 99,9 % de disponibilité mensuelle :
Au-delà des quarante (40) premières minutes d'indisponibilité cumulée du mois en cours, une pénalité de dix pour cent (10 %) du montant de l'abonnement mensuel par tranche de vingt (20) minutes d'indisponibilité, dans la limite de cent pour cent (100 %) du montant de l'abonnement mensuel.

Article 3.3 – Conditions de mise en œuvre

Le Client doit notifier à CASTLE IT sa demande d'application des pénalités dans un délai de dix (10) jours calendaires suivant la fin du dysfonctionnement.

Les pénalités de service sont la seule sanction convenue en cas d'incident portant sur la disponibilité des services. Le client renonce en conséquence dès à présent à former toutes autres réclamations indemnitaires.

Article 4 – Conditions d'accès et notification des incidents

Article 4.1 – Déclaration par le Client

Le Client peut signaler tout incident ou défaut de fonctionnement 24 heures sur 24 et 7 jours sur 7 :

- par téléphone au numéro unique d'astreinte : 06.50.87.04.69 (tout appel injustifié pourra être facturé cinquante (50) euros HT),
- par ticket via l'interface client : <https://customers.castle-it.fr>
- par ticket via l'interface Nova Links : <https://nova.castle-it.fr>

Article 4.2 – Notification par CASTLE IT

CASTLE IT s'engage à notifier au Client, par tout moyen approprié, tout incident de sécurité ou d'indisponibilité détecté par ses systèmes de supervision dans un délai maximum de deux (2) heures suivant sa détection.

Article 4.3 – Maintenance planifiée

Les périodes de maintenance planifiée, notifiées au Client avec un préavis minimum de vingt-quatre (24) heures, ne sont pas prises en compte dans le calcul de la disponibilité contractuelle. CASTLE IT s'engage à limiter la durée et l'impact des opérations de maintenance planifiée.