

CHARTRE D'ACCES AU SI POUR LES FOURNISSEURS

Identification du document	
Référence	P2-4-PRESTA01-01_CHARTRE D'ACCES AU SI POUR LES FOURNISSEURS ET PRESTATAIRES
Date de dernière mise à jour	24/10/2020
Version	V1.0
Classification	Confidentiel
Nombre de pages	14

Etablissements de santé du GHT 78 Sud

CYCLE DE VIE DU DOCUMENT

AUTEUR(S)		
Fonction	Nom	Date
RSSI	Antoine Toutain	23/10/2019

RELECTEUR(S)		
Fonction	Nom	Date
DSI GHT 78 Sud	Stéphane Harnisch	29/04/2021
RSI GHT 78 Sud	Hervé Paris	10/02/2021

VALIDATION		
Fonction	Nom	Date
DSI GHT 78 Sud	Stéphane Harnisch	29/04/2021

HISTORIQUE DU DOCUMENT

Version	Date	Description	Détails
R 01	23/10/2020		

Etablissements de santé du GHT 78 Sud

1. Objet

La présente charte s'inscrit dans une démarche d'information, de sensibilisation et de responsabilisation des Fournisseurs afin de poser les règles d'accès et d'utilisation des Systèmes d'Information de l'ensemble des SI des établissements membres du GHT 78 Sud.

Elle a pour objet de définir les conditions et modalités que le fournisseur s'engage à respecter afin d'assurer la sécurité des SI du CH du GHT ainsi que de ses données. L'objectif consiste ainsi à éviter que les relations avec les fournisseurs ne constituent une faille dans les règles de sécurité informatique définies par le Responsable Sécurité Système d'Information (RSSI) et la direction des SI (RSI/DSI GHT).

Cette charte et les règles qu'elle contient ont été établies en application de la Politique de Sécurité du Système d'Information (PSSI) du GHT 78 Sud et sous l'autorité du DSI et du RSSI du GHT 78 Sud.

Elle fait partie du référentiel de sécurité du GHT approuvé par la Direction Générale de l'établissement support. Elle est partie intégrante de tout Marché liant le fournisseur à l'établissement du GHT.

Son respect constitue une obligation essentielle à la charge du fournisseur.

Personnel concerné	Lieux de diffusion
Fournisseurs	SI/ACHATS SI /MARCHE SI

2. Domaine d'application

Cette charte s'applique à toute prestation pour lequel le fournisseur accède au SI d'un CH du GHT. Le fournisseur a l'obligation de se conformer à ses dispositions, cette charte étant annexée à une pièce opposable du marché.

Elle s'applique à compter de la date de publication mentionnée sur la page de garde de ce document.

Ses dispositions sont applicables dès la notification du marché à laquelle elle est annexée. Elle reste en vigueur pour toute la durée du marché. Comme tout utilisateur du Système d'Information du GHT tout fournisseur est soumis à la Charte d'Accès et d'Usage du SI.

La présente Charte Fournisseurs décrit les dispositions spécifiques aux fournisseurs vis-à-vis des SI des établissements membres du GHT.

3. Définitions

« Système d'information (SI) » : On entend par Système d'Information (ci-après le « SI ») l'ensemble des ressources, matérielles et logicielles, des moyens techniques, et des procédures et moyens

Etablissements de santé du GHT 78 Sud

humains et organisationnels, mis en jeu dans la création, le stockage, le traitement, l'archivage, la transmission, la diffusion et la communication des données et informations utilisées dans le fonctionnement de l'entreprise.

Cela inclut entre autres : les logiciels (applications informatiques, systèmes de messagerie électronique, outils bureautiques, systèmes d'exploitation, outils d'administration, utilitaires, bases de données, solutions bio médicales connectées au SI...), les matériels informatiques ou bureautiques (serveurs, ordinateurs et téléphones – fixes ou portables –, PDA, imprimantes et photocopieurs, etc.), les équipements des réseaux de données (routeurs, commutateurs, autocommutateurs, fax...), les médias de stockage (disques durs, CD-ROM, clés USB, ...) et les équipements de production.

« Marché » : Contrat de prestations de services, de fournitures de matériels ou de logiciels / progiciels, de travaux, etc., liant contractuellement, au sens du Code des Marchés Publics, un fournisseur au GHT 78 Sud ou un de ses établissements membre (la présente charte est annexée au marché).

« Fournisseur » : Titulaire du marché auquel est annexée la présente charte, ainsi que ses éventuels sous-traitants dont il fait son affaire et pour lesquels il s'engage.

« DSI » : Direction des Systèmes d'Information du GHT.

« RSI » : Responsable des Systèmes d'Information du GHT.

« RSSI » : Responsable Sécurité des Systèmes d'Information du GHT.

« CH » : Centre hospitalier ou tout établissement de santé membre du GHT 78 Sud.

4. Description du document

4.1 Généralités

- L'ensemble des informations et des documents fournis par le CH du GHT, quel que soit leur support, reste la propriété exclusive, pleine et entière du CH du GHT. Le fournisseur devra en assurer la protection et respecter la non-divulgateion de leur contenu.
- Il ne pourra en aucun cas procéder à des démonstrations ou toute autre exploitation utilisant ces informations à d'autres fins que celles pour lesquelles elles lui ont été transmises, en particulier réutiliser les bases de données du CH du GHT afin d'en récupérer le paramétrage technique ou fonctionnel pour d'autres marchés.
- Quel que soit le support, **le Fournisseur doit considérer par défaut comme confidentiel l'ensemble des informations, documents et toute autre donnée qu'il reçoit du CH, traite ou crée pour son compte.** Plus particulièrement, le Fournisseur s'engage à ne pas divulguer les informations recueillies sur les faiblesses et les vulnérabilités du SI du CH, ainsi que toutes

Etablissements de santé du GHT 78 Sud

les données à caractère personnel, les informations confidentielles ou médicales dont il aura pu avoir connaissance au cours de sa mission.

- Le Fournisseur doit veiller à la sécurité des Ressources informatiques qu'il détient en assurant, en interne et vis-à-vis des tiers, la confidentialité, la disponibilité, la pérennité et l'intégrité des informations. Ces informations sont strictement couvertes par le secret professionnel conformément à l'article 226-13 du code pénal.
- A ce titre, le Fournisseur prendra vis-à-vis de son personnel toutes les mesures nécessaires pour qu'il respecte le secret et la confidentialité de toutes les informations et de tous les documents appartenant au CH. Pour ce faire, le Fournisseur s'engage à faire signer à chaque membre de son Personnel intervenant dans les prestations pour le CH, une copie de la présente charte.
- Le Fournisseur reste seul juge des différents moyens qu'il lui appartient de mettre en œuvre pour assurer et garantir la sécurité des informations et des ressources appartenant au CH. Toutefois, le Fournisseur s'engage à respecter les obligations suivantes et à les faire respecter par son Personnel :
 - N'effectuer aucune copie des documents et des ressources informatiques confiés par le CH, à l'exception de celles nécessaires à l'exécution de sa mission.
 - Prendre toutes les mesures de sécurité, notamment matérielles, pour assurer la conservation, l'intégrité, la pérennité et la confidentialité des documents et des informations traitées pendant l'exécution des prestations quel que soit le support utilisé ;
 - En fin de marché, et ce pour quelque cause que ce soit, procéder à la restitution immédiate de tous les documents, les données et les Ressources informatiques appartenant au CH ou, à défaut, procéder à la destruction sécurisée de chacun des supports et de chacune des informations non restituées ; à ce titre le CH pourra demander que la destruction des données s'effectue en sa présence ou demande des preuves matérielles de cette destruction de données ;
- Le Fournisseur s'engage à n'exécuter aucun autre traitement que ceux prévus contractuellement sur les informations et les données fournies par le CH ou leurs résultats. Le traitement doit être proportionné et conforme à la finalité prévue dans le Marché signé avec le CH, à la présente charte et aux règles générales relatives à la sécurité du Système d'information du CH.
- Le Fournisseur s'interdit l'utilisation des Ressources informatiques mises à sa disposition par le CH à des fins autres que celles figurant dans le Marché.

4.2 Cas particulier d'accès aux données médicales

- Au cas où le Fournisseur serait en position d'accéder à des données médicales nominatives, il est rappelé que les dispositions juridiques en vigueur imposent pour l'accès à ces données d'un moyen d'authentification forte.

Etablissements de santé du GHT 78 Sud

- Le CH souhaite mettre particulièrement l'accent sur le caractère sensible des données médicales nominatives, et demande au Fournisseur de mettre en place tous les moyens à sa disposition afin de respecter les dispositions réglementaires en vigueur.
- En particulier, le Fournisseur devra porter un soin particulier à l'accès à ces données médicales nominatives lors d'opérations de télémaintenance. Le Fournisseur devra prendre toutes les dispositions nécessaires pour qu'en aucun cas les données médicales ne sortent du CH.

4.3 Copies des bases de données du CH

- Qu'il s'agisse de maintenance technique ou autre, toute copie de données du CH est soumise à stricte autorisation de la DSI et du RSSI.
- Un fournisseur qui copierait des données du CH sans autorisation formelle s'exposerait à des poursuites immédiates.

5. Accès Physiques

5.1 Accès physiques aux locaux

- L'accès aux locaux se fait à l'aide de badges d'identification.
- Les salles où le Fournisseur est hébergé ainsi que les moyens d'accès physiques lui sont communiqués par le CH. Le Fournisseur s'engage à suivre les règles suivantes :
 - Ne pas essayer de s'introduire dans des salles non autorisées ou avec d'autres moyens que ceux mis à sa disposition ;
 - Ne pas permettre l'accès aux personnes non autorisées par le CH dans les locaux du CH ;
 - Respecter les systèmes de sécurité physique mis en place au CH, en particulier fermer systématiquement à clé s'il le peut, les portes derrière lui, même en cas d'absence de courte durée ;
 - Assurer la protection physique du matériel mis à sa disposition ;
 - Restituer tous les objets permettant l'accès physique aux infrastructures et prêtés par le CH durant la prestation du Fournisseur (cartes, clés, etc.) à la fin de l'intervention ;
 - Ne réaliser aucune copie ou duplicata des moyens d'accès mis à disposition ;
 - Ne pas entraver le fonctionnement des équipements opérationnels et ceux de sécurité ;
- Dans le cas des opérations de maintenance (par exemple, réparation matérielle), le Fournisseur doit transmettre au préalable ou dans les plus brefs délais au CH un descriptif précisant les dates, la nature des opérations à effectuer et les noms des intervenants.
- Dans le cas de la livraison d'une solution ou de matériel (par exemple : stock informatique, papiers, mobilier), il est toléré que l'accès du bâtiment soit provisoirement ouvert. Un membre habilité de la DS2I, à défaut le Fournisseur, est chargé de veiller à la fermeture systématique du bâtiment dès la livraison terminée.

Etablissements de santé du GHT 78 Sud

- Seul le Personnel affecté aux missions définies dans le Marché signé avec le CH pourra avoir accès aux clés, codes, matériels ou locaux utilisés pour assurer la protection physique des informations et Ressources informatiques appartenant au CH.
- Chaque membre du Personnel ayant accès à ces clés ou codes s'engage à les garder secrets, à ne pas les dévoiler ou les laisser à la disposition des tiers. Il s'engage également à ne pas laisser les matériels à la disposition des tiers.
- Par ailleurs, afin d'assurer la sécurité des biens ou des personnes, certains sites sensibles ont été équipés de procédés de vidéosurveillance. Le Fournisseur reconnaît être informé que de tels systèmes ont été mis en place dans les sites sensibles. Le CH s'engage à respecter la législation applicable à ce type d'équipement.
- De même, toujours afin d'assurer la sécurité des biens et des personnes, le CH limite l'accès à certaines zones sensibles au moyen d'un système de contrôle par badge donnant lieu à un traitement de données à caractère personnel. Ainsi, tout membre du Personnel du Fournisseur ayant une habilitation peut accéder à des lieux précis selon le type et le niveau d'habilitation dont il bénéficie. Le CH s'engage à respecter la législation relative aux traitements de données à caractère personnel mis en place à cette fin.

5.2 Connexion du matériel du Fournisseur sur le réseau

- Dans la majorité des cas, l'utilisation de matériels informatiques fournis par le CH doit être privilégiée.
- Dans le cas où le Fournisseur aurait besoin, pour l'exécution de sa prestation, de connecter des matériels informatiques lui appartenant sur le réseau du CH, cette connexion est possible aux conditions suivantes :
 - Respect de la Charte d'Utilisation du Système d'Information ;
 - Respect des différentes mesures spécifiques de sécurité du CH ;
 - Intégration du matériel au domaine Active Directory si nécessaire ;
 - Présence d'un antivirus ou d'une solution de sécurité adaptée à jour.
 - Présence d'un Système d'Exploitation de type Microsoft Windows 10 ou version ultérieure validée par la DSI, à jour en termes de patch de sécurité et à même de récupérer au moins 1 fois par semaine les derniers patchs de sécurité Microsoft ;
 - Respect des contraintes d'adressage MAC et IP de la DSI ;
 - Le Fournisseur devra démontrer que son matériel ne présente aucun risque de compromission ou d'infection du réseau informatique du CH ;
 - Cette connexion ne doit en aucune manière avoir un impact sur les performances, la disponibilité, l'intégrité et la confidentialité du Système d'Information du CH ;
 - Le matériel doit se connecter au réseau du CH par les modalités définies par l'établissement (Switch, prises RJ45, etc.) ; les connexions à l'aide de modem sont interdites ;
- **Le Fournisseur s'engage à ne connecter aucun matériel informatique sans l'accord explicite et écrit de la DSI du CH ou du RSSI.**

Etablissements de santé du GHT 78 Sud

6. Accès Logiques

6.1 Généralités

- Tout accès logique au Système d'Information du CH nécessite au préalable :
 - L'attribution par la DSI d'un compte utilisateur Active Directory nominatif (en première intention de type profil à « moindre privilège ») lorsque cela est nécessaire, actif pour le temps exclusif de la prestation et / ou de la connexion ;
 - Attribution éventuelle de moyens d'authentification forte de type carte à puce, de façon nominative et pour le temps exclusif de la prestation ;

Ces comptes utilisateurs peuvent être nominatifs (individuels) ou collectif en fonction du domaine, des besoins et de la législation.

6.2 Sécurité des accès logiques

- Il appartient au Titulaire de s'assurer de la bonne utilisation des comptes utilisateurs qui lui ont été fourni, et en particulier :
 - Garantir que ces codes d'accès ne sont accessibles qu'aux personnels autorisés ;
 - S'assurer de la mise à jour régulière des personnels autorisés, notamment suite à des départs éventuels de personnels chez le Titulaire ; les accès adéquats devront être révoqués en cas de cessation du besoin et / ou de départ du personnel concerné ;
 - Traiter ces informations de connexion comme des informations hautement confidentielles, engagement pour lequel le Titulaire est soumis à une obligation de résultats ;
 - Assurer de façon générale la protection contre tout accès non autorisé par tous les moyens adéquats (protection péri métrique, protection physique, etc.).
- Le Fournisseur et son Personnel s'engagent à :
 - Faire respecter la protection, la non-divulgaration et le non-partage du mot de passe des intervenants qui doivent en assurer une utilisation strictement personnelle. Le mot de passe est inaccessible et doit être suffisamment robuste ;
 - Communiquer au CH, dès l'ouverture des autorisations d'accès au système et en cas de changement, le nom des intervenants et l'identification utilisateurs associés ;
 - Ne pas user de leur droit pour accéder à des applications, à des données ou à un compte informatique autres que ceux qui leur auront été éventuellement attribués ou pour lesquels ils ont reçu l'autorisation d'accès ;
 - Ne pas user, par quelque moyen que ce soit, du droit d'accès d'un autre utilisateur ;
 - Ne pas altérer ou détruire des traces ou preuves relatives à des actions ou des événements sur les Système d'Information du CH, le concernant ou non ;
 - Ne pas entraver le fonctionnement des équipements opérationnels et ceux de sécurité et dans tous les cas ne pas porter atteinte à la production informatique du CH ;
- Le Personnel du Fournisseur devra avertir la DSI de tous dysfonctionnements constatés et/ou de toutes anomalies générées de son fait ou ne le concernant pas mais relevant de la sécurité, qu'il aura pu observer lors de l'exécution de ses prestations. A cet égard, la procédure d'alerte

Etablissements de santé du GHT 78 Sud

consiste à prévenir par tout moyen et dans les plus brefs délais la DSI ou le RSSI, qui s'attachera à isoler le dysfonctionnement.

6.3 Protection contre les logiciels malveillants

- Ce paragraphe fait référence aux virus, spyware, codes toxiques, etc., c'est-à-dire à tout malware ou logiciel malveillant.
- Toutes les solutions, qu'elles soient logiques ou physiques, doivent s'intégrer dans la stratégie antivirale du CH.
- Les machines introduites sur le réseau devront avoir une protection antivirale ou un dispositif de sécurité (identiques fonctionnellement à ceux du CH) à jour de façon à éviter la contamination des SI ; étant noté que l'utilisation d'un quelconque outil ou matériel sur le réseau est interdite, sauf accord préalable de la DSI ou du responsable du service concerné.
- De même, tous les supports de stockage mobiles (clés USB, CD-ROM, etc.) ne pourront être utilisés sur un équipement du CH qu'après accord de la DSI et devront avoir été balayés (ou examiner via une station de décontamination), en présence d'un agent de la DSI, par un antivirus à jour. Le Fournisseur s'engage à procéder de même pour l'utilisation de tels supports sur son propre matériel.
- Lorsque le Fournisseur intervient sur site, le CH se réserve le droit d'installer eux-mêmes un antivirus sur les machines utilisées par le Fournisseur dans le cadre de sa prestation afin d'effectuer le scan de chaque poste et des supports d'information.

7. Télémaintenance

7.1 Généralités

- La télémaintenance est nécessaire au bon maintien en condition opérationnelle de beaucoup d'équipements utilisés par le CH.
- Elle se divise en 2 cas d'utilisation :
 - Cas 1 : le fournisseur se connecte, depuis l'extérieur du CH, à un équipement situé sur le LAN ou dans la DMZ du CH ; il s'agit de télémaintenance à proprement parlé ;
 - Cas 2 : le fournisseur a positionné sur le LAN du CH un équipement qui envoie des informations techniques (logs, traces, alertes, etc.) à un équipement du fournisseur situé en dehors du LAN ; ce cas d'usage s'apparente à de la supervision ;

7.2 Connexion depuis l'extérieur

Etablissements de santé du GHT 78 Sud

- Aucun accès par modem n'est autorisé : tous les accès au système d'information du CH depuis l'extérieur devront passer par les équipements et des solutions de sécurité validée par la DSI : (VPN, ZTNA, Bastions).

La solution de télémaintenance proposée par le fournisseur devra répondre aux exigences de sécurité de la DSI et du RSSI, la DSI peut refuser un moyen de connexion qui ne répondra pas à ses critères.

- De plus :
 - Aucun accès en télémaintenance n'est ouvert en permanence (hors contrat d'infogérance) ;
 - Tout accès en télémaintenance sur un équipement de production doit passer par une ouverture manuelle de l'accès (**accusé**), charge à la DSI de déterminer le workflow optimal ;
 - L'ouverture d'un accès en télémaintenance doit avoir une durée limitée à la durée de l'intervention ;
 - Dans un cas d'urgence, un accès en télémaintenance sur un équipement en production peut shunter les phases de tests, l'urgence doit être motivée auprès d'un agent habilité de la DSI ;
 - Dans tous les autres cas (ceux qui ne relèvent pas de l'urgence), aucun accès en télémaintenance en production qui n'ait pas été précédé par une phase de qualification (sur un environnement de test ou sur l'environnement de production cible), et explicitement validé par un agent habilité de la DSI et le RSSI ;
 - il est nécessaire de tracer nominativement les personnes des sociétés extérieures qui accèdent en télémaintenance ; les comptes nominatifs sont un moyen idéal, mais il est possible d'utiliser dans des situations exceptionnelles des comptes génériques sous réserve de la mise en place d'un fonctionnement de type « main courante » avec trace écrite informatisée, idéalement à la charge du fournisseur ;
- En cas de télémaintenance permettant l'accès à distance aux ressources du SI du CH, le Fournisseur devra obligatoirement :
 - Obtenir l'accord préalable du CH avant chaque opération de télémaintenance dont il prendrait l'initiative. En particulier les accès à la production sont strictement interdits, sauf accord explicite de la part de la DSI. Il en va de même pour les environnements d'intégration ;
 - Prendre toutes dispositions afin de permettre au CH d'identifier la provenance de chaque intervention extérieure ;
 - Transmettre systématiquement au chef de projet ou responsable de l'application un rapport de télémaintenance retraçant les opérations menées, les modifications réalisées sur l'environnement de production et leurs impacts éventuels, et ce quels que soient les composants modifiés (système, applications, middlewares, réseaux) ;
 - S'assurer de l'intégrité de son poste, de la mise à jour de celui-ci par rapport aux derniers patches sécurité et protection contre les codes malveillants (antivirus, antimalware ...) ;
 - Ne pas se connecter à des sources concurrentes potentiellement compromettantes telles qu'Internet, autres réseaux d'accès distant, etc. ;
 - Mettre en application l'ensemble des pratiques permettant d'assurer la sécurité de l'accès distant et des outils associés, et se plier aux contraintes techniques imposées par la DSI,

Etablissements de santé du GHT 78 Sud

notamment sur les moyens techniques de chiffrement des communications à utiliser pour éviter la transmission des données en clair ;

- En particulier, l'accès en télémaintenance par le fournisseur à un serveur de production contenant des données réelles doit être une exception. L'accès en télémaintenance à un serveur de tests ou de pré-production doit être privilégié, afin de réaliser les opérations techniques qui seront ensuite répercutées sur l'environnement de production.
- L'accès en télémaintenance à un serveur de production ne se justifie que dans un cas d'urgence, avec approbation écrite de la DSI et sous contrôle de celle-ci.
- En ce qui concerne l'accès par le fournisseur aux postes de travail des agents du CH :
 - Cet accès est exceptionnel, et délivré par le CH pour une durée ne pouvant excéder la durée d'exécution du marché ;
 - Tout usage de cet accès doit faire l'objet d'une demande d'intervention auprès d'un agent habilité de la DSI (qui en assurera le suivi) ;
 - En aucun cas cet accès ne constitue un droit de visualiser des données confidentielles (données médicales par exemple) ; à ce titre le fournisseur devra limiter son intervention aux strictes opérations nécessaires pour assurer sa mission ;
 - Tout manquement aux règles de confidentialité et de déontologie engage la responsabilité juridique du fournisseur ;
 - Tous les accès sont susceptibles d'être tracés ;

8. Spécificité dans les interventions

8.1 Généralités

- Toute intervention sur le SI du CH, que ce soit à distance ou sur site, présente des risques inhérents de perturbation dans le fonctionnement des applications.

8.2 Engagements du Fournisseur

- La récupération des flux et autres actions visant à tester la robustesse des Systèmes d'Information sont interdites (excepté en cas de demande préalable et explicite du CH : audit, tests d'intrusion, tests de montée de charge, validation de performance, etc.).
- Par ailleurs, le Fournisseur s'engage à ne pas se servir du réseau du CH pour présenter une solution ou procéder à de l'avant-vente. Pour de telles démonstrations, il devra mettre en place sa propre architecture.
- En particulier, il est strictement interdit au Fournisseur d'utiliser le réseau du CH afin de procéder à une démonstration (par exemple de la nouvelle version d'un progiciel déjà détenu par le CH, ceci n'étant qu'un exemple) directement dans un service utilisateur et sans passer par le point de contact unique qui est la DSI, qui devra avoir explicitement et par écrit autoriser une telle utilisation.

Etablissements de santé du GHT 78 Sud

8.3 Incidents

- Le Fournisseur s'engage à informer immédiatement le CH de tout évènement pouvant affecter la disponibilité, l'intégrité, la pérennité, la confidentialité ou la perte d'informations du CH qu'il détient, auxquelles il accède où qu'il manipule.

9. Audits, Traçabilités et Contrôles

9.1 Généralités

- Tout accès au SI du CH est tracé, conformément aux lois Informatique et Libertés. Ces traces sont conservées 1 an.

9.2 Traçabilité des accès

- Il appartient au Titulaire, dans le cas de l'attribution d'un compte utilisateur générique (c'est-à-dire affecté au Titulaire et non pas nominativement à un ou plusieurs employés) de gérer la traçabilité des accès.
- La Personne Publique doit, sur simple demande, pouvoir disposer de l'historique nominatif de l'utilisation de cet accès générique, s'entend quel employé du Titulaire a utilisé cet accès, à quelles dates et heures, pour quelle durée et pour quelle action.

10. Aspects Juridiques

10.1 Responsabilité

- Le Fournisseur est responsable de tous les dommages corporels, matériels et immatériels, directs ou indirects, trouvant leur origine aussi bien dans une exécution fautive, même partielle ou une mauvaise exécution ou une inexécution des obligations mises à sa charge dans la présente charte.
- Le Fournisseur est seul responsable du respect des présents engagements et de leur mise en œuvre ainsi que de leur respect par son Personnel.
- Nonobstant sa responsabilité contractuelle, le Fournisseur est informé que selon la faute commise, sa responsabilité civile (par exemple pour atteinte au droit à l'image d'un tiers) et/ou pénales (par exemple pour intrusion frauduleuse dans les SI ou pour violation du secret professionnel) pourra être engagée.

10.2 Respect des lois en vigueur

Etablissements de santé du GHT 78 Sud

- Le Fournisseur s'engage non seulement au respect de la présente charte, mais déclare également connaître et respecter la réglementation en vigueur et notamment à titre non limitatif :
 - La loi 78-17 du 6 janvier 1978 modifiée par la loi du 4 août 2004 relative à l'informatique, aux fichiers et aux libertés et ses textes d'application ;
 - Les dispositions du code pénal relatives à la fraude informatique (articles 323-1 à 323-7 du Code pénal) ;
 - Les dispositions du code civil relatives aux atteintes aux droits de la personne (notamment atteintes à l'intimité de la vie privée et au droit à l'image) ;
 - Les dispositions du code pénal relatives aux atteintes aux droits de la personne (notamment, atteintes à la vie privée, au secret des correspondances privées, atteintes au secret professionnel et atteintes résultant de fichiers ou de traitements informatiques) ;
 - Les dispositions du code de la propriété intellectuelle relatives au droit d'auteur (les logiciels, toutes les œuvres de l'esprit quelle que soit leur nature, les bases de données), aux brevets, aux marques et aux dessins et modèles ;

10.3 Intitulé des clauses

- Les intitulés portés en tête de chaque article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

10.4 Invalidité d'une clause

- Si une ou plusieurs stipulations de la présente charte sont tenues pour non valides ou déclarées telles en application d'une loi, d'un règlement ou à la suite d'une décision définitive d'une juridiction compétente, les autres stipulations conserveront leur pleine validité sauf si elles présentent un caractère indissociable avec la stipulation non valide.

10.5 Exceptions

- Chaque cas d'exception appelant une dérogation à la présente charte devra systématiquement être soumis à la DSI pour identification, validation et suivi

11. Entrée en vigueur de la charte

- La présente charte sera applicable, à compter de la date de publication mentionnée sur la page de garde du document.

12. Signature du fournisseur

Je, soussigné :

Etablissements de santé du GHT 78 Sud

Représentant de la société :

Déclare accepter sans réserve les conditions du présent document.

Fait à :

Le :

Signature (précédée de la mention « lu et approuvé »)