



|  |
| --- |
| Charte du bon usage des technologies numériques |
| Volet Prestataires |
| DSI, Département Méthode, Qualité, Sécurité et Contrôle Interne |
| Version document : 21/04/23 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Réf. Modèle | Réf. Documentaire | Version | Appliqué(e) le |
| 06- Document (2 signatures) | 001 | 26888 | 002 | 09/05/2023 |
|  | Rédaction | | Approbation | |
| Nom(s) et fonction(s) | Cedric HAMELIN (Gedi : Rédacteur - CHU\Pôles - Directions\Directions Administratives\Direction du Système Information\Architecture et Sécurité du Système d'Information) | | Laure AMAND (Gedi : Approbateur - CHU\Pôles - Directions\Directions Administratives\Direction du Système Information) | |
| Date | 02/05/2023 09:09:20 | | 04/05/2023 12:27:50 | |

**Charte du bon usage des technologies numériques**

Volet Prestataires

**SOMMAIRE**

[A. Objet 2](#_Toc133493452)

[B. Objectifs 2](#_Toc133493453)

[C. Cadre réglementaire – Documents de référence 3](#_Toc133493454)

[D. Dispositions administratives générales 3](#_Toc133493455)

[E. Consignes de sécurité pour le personnel du fournisseur 3](#_Toc133493456)

[F. Règles régissant les interventions 4](#_Toc133493457)

[G. Accès physique sur site 4](#_Toc133493458)

[H. Accès distant au système d’information 4](#_Toc133493459)

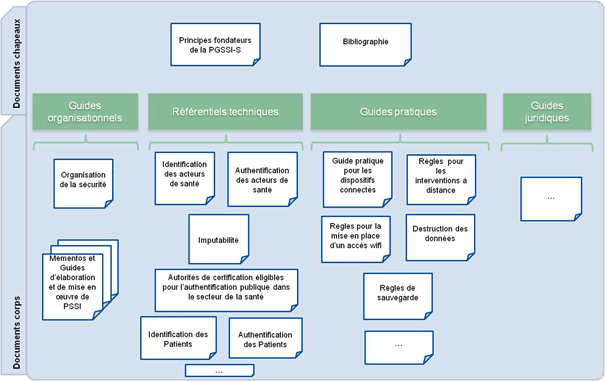
[I. Dispositions particulières pour la sécurité du système d’information 5](#_Toc133493460)

[ANNEXE 1 : ENGAGEMENT PERSONNEL DU FOURNISSEUR / PRESTATAIRE 6](#_Toc133493461)

1. Objet

Ce document présente la **Charte Prestataire** du Centre Hospitalier Universitaire (CHU) de Rouen.

Ce document est un élément complémentaire de la **Politique de Sécurité des Systèmes d’Information** (référence GEDI :[26261](http://thot:8080/eDoc/actions/redirect?method=attachment&ref=26261&datasource=ennovged&workspace=intranet)), document fondateur de la démarche de sécurisation des systèmes d’information CHU-Hôpitaux de Rouen. Il fait partie des référentiels spécifiques définis dans la Politique Générale de Sécurité des Systèmes d’Information de Santé ([PGSSI-S](http://esante.gouv.fr/services/referentiels/securite/pgssi)).



La Charte prestataire a pour objet de sensibiliser les intervenants extérieurs au respect des règles de confidentialité et des règles permettant d’assurer la sécurité et la performance du Système d’information de l’Etablissement.

Elle décrit les règles de sécurité relatives aux interventions de tiers fournisseurs ou prestataires de services télécoms.

En signant cette charte, le fournisseur ou prestataire reconnait en avoir pris connaissance et s’engage librement à en appliquer strictement le contenu.

1. Objectifs

La charte est systématiquement annexée au cahier des charges pour l’acquisition de matériels, logiciels, systèmes ou solutions en relation avec le Système d’Information. Elle doit donc être signée préalablement à la notification du marché.

Le document est un prérequis dans la validation des accès au Système d’Information de l’établissement pour les intervenants du fournisseur.

Cette charte doit être signée par un responsable (Directeur, Directeur Adjoint, Directeur Commercial ou Responsable Opérationnel) du fournisseur ou nominativement par chacun des intervenants du fournisseur.

Pour les prestataires déjà sous contrat, la charte doit être également signée, lors d’un renouvellement de contrat ou de changement d’intervenant par exemple.

Elle s’applique également aux systèmes d’information des équipements biomédicaux et tous équipements connectés (réseau, téléphonie, imprimantes, …).

1. Cadre réglementaire – Documents de référence

* Loi Informatique et Libertés :

La loi Informatique et Libertés est applicable dès lors qu’il existe un traitement, automatisé ou manuel, contenant des informations relatives à des personnes physiques.

Elle définit les principes à respecter lors de la collecte, du traitement et de la conservation de ces données et garantit un certain nombre de droits pour les personnes.

* [PGSSI-S](http://esante.gouv.fr/services/referentiels/securite/pgssi) – Guide ASIP-Santé « Règles pour les interventions à distance sur les systèmes d’information de santé » – Décembre 2014 – V1.0 :

Ce guide définit les règles et les recommandations de sécurité relatives aux interventions effectuées à distance sur un système d’information de santé. Il détaille les règles de sécurité auxquelles doivent se conformer, au sein des structures juridiques utilisatrices de systèmes d’information de santé, les acteurs responsables de la mise en place et du suivi de prestations effectuées à distance. Certaines règles sont destinées à être appliquées par les fournisseurs des interventions à distance.

* CCAG-TIC - Cahier des Clauses Administratives Générales-Techniques de l’Information et de la Communication :

Ce document est le cahier des clauses administratives générales applicables aux marchés publics de technologies de l'information et de la communication, approuvé par l’arrêté du 16 septembre 2009. Son utilisation garantit des engagements contractuels clairs et sécurisés en reprenant notamment l’ensemble des clauses communes aux différents CCAG, principalement les obligations générales des parties, les dispositions relatives au développement durable, l’obligation d’assurance, les dispositions en matière de livraison, de transport, de stockage et les clauses de résiliation.

1. Dispositions administratives générales

Toutes les prestations réalisées le sont soit à partir de la zone de l’Union Européenne, soit en respectant les règles définies par la CNIL pour les prestations hors zone de l’Union Européenne (<http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/>).

Le fournisseur de prestations informatiques se réfère au CCAG TIC : <http://www.marche-public.fr/Marches-publics/Textes/CCAG/CCAG-TIC/CCAG-TIC.htm>.

Le fournisseur est tenu de déclarer tout changement relatif à sa situation administrative. Cette déclaration peut être mise à disposition, via internet sur l’espace client du site du fournisseur, associée à une notification des clients par message électronique.

Le fournisseur informe, dès la signature du contrat, l’Etablissement de la possibilité d’utilisation de la sous-traitance. En cas de recours à la sous-traitance, le fournisseur répercute les exigences qui lui sont applicables vers le sous-traitant, sous son entière responsabilité.

1. Consignes de sécurité pour le personnel du fournisseur

Le fournisseur s’engage vis-à-vis de la confidentialité des informations auxquelles son personnel peut avoir accès. Chaque personne concernée (intervenant sur site ou à distance) signe un engagement individuel de confidentialité annexé au contrat entre le fournisseur et l’Etablissement.

Le fournisseur s’engage vis-à-vis des actions que son personnel peut effectuer. Chaque personne concernée doit avoir signé un engagement individuel de limitation de ses actions au seul besoin des interventions.

Le fournisseur doit sensibiliser les personnes autorisées, à la sécurisation des accès (physiques et logiques) des postes d’intervention tant à distance que sur site client et fournir le cas échéant les postes d’intervention et les moyens de sécurité associés.

1. Règles régissant les interventions

Le fournisseur s’engage formellement à :

* ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l’exception de celles nécessaires à l’exécution de la présente prestation prévue au contrat, l’accord préalable du propriétaire du fichier est nécessaire ;
* ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
* ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
* prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
* prendre toutes mesures de sécurité, notamment matérielle, pour assurer la conservation et l’intégrité des documents et informations traités pendant la durée du présent contrat ;
* et en fin de contrat procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

1. Accès physique sur site

Tout fournisseur doit connaître et appliquer les politiques, procédures et standards de sécurité de l’établissement lorsque celui-ci intervient dans les locaux de l’établissement de santé ou lors de la fourniture de service informatique (mise à disposition de matériel informatique, accès logique, etc.).

Les règles d’accès sont les suivantes :

* Toute intervention est nécessairement planifiée au travers d’un processus impliquant une demande d’autorisation préalable.
* Lors d’un accès sur site, le personnel du fournisseur est accompagné sur site en zone sensible par un personnel habilité de la DSI ou des services techniques.
* Les travaux réalisés et l’éventuelle remise en état avant de quitter le site, font l’objet d’un procès-verbal de la part de la DSI pour les opérations sensibles.

Le fournisseur s’engage à respecter les procédures et processus définis par l’établissement pour accéder aux informations qui lui sont nécessaires pour remplir ses fonctions. Il s’engage aussi à ne pas essayer d’outrepasser les mesures et contrôles d’accès en place, pour quelque raison que ce soit.

1. Accès distant au système d’information

Le fournisseur doit fournir une liste nominative actualisée des personnes pouvant solliciter une intervention à distance et s’engage donc à tenir informé l’établissement de tout retrait de personnes afin que les accès soient désactivés.

Le fournisseur doit assurer la sécurité de sa plateforme d’intervention à distance, des points de vue accessibilité, protection des données et des logiciels.

Le fournisseur doit restreindre les accès logiques des postes d’intervention aux seules personnes autorisées.

Le fournisseur doit restreindre autant que faire se peut les accès physiques des postes d’intervention aux seules personnes autorisées.

S’il le désire, le Directeur des Systèmes d'Information a la possibilité de faire réaliser des contrôles des dispositions de sécurité prises par le fournisseur pour la réalisation de sa prestation.

Le fournisseur doit être en mesure de déterminer en toute circonstance l’identité de toute personne qui se connecte ou s’est connectée sur sa plateforme et en assurer la traçabilité.

Le fournisseur doit mettre en œuvre des moyens et des procédures conformes aux règles de l’art, pour lutter contre les incidents pouvant affecter la sécurité du système de l’établissement ou ses informations ou la sécurité de l’intervention elle-même. Cette exigence concerne :

* la lutte contre les incidents de sécurité dans l’environnement humain, organisationnel, technique ou physique du fournisseur et pouvant affecter la sécurité de la prestation fournie ;
* la lutte contre les codes malveillants et contre l’exploitation de vulnérabilités connues, dans les moyens informatiques ou de télécommunication mis en place pour la prestation dans le système d’information, sous la responsabilité du fournisseur.
* la lutte contre la propagation de codes malveillants ou d’incidents de sécurité à partir de la plateforme du fournisseur, au travers des échanges électroniques effectués au titre de la prestation ;
* la lutte contre les codes malveillants dans les logiciels transmis au titre de la prestation ou dans leur mise à jour, et contre l’exploitation de vulnérabilités connues dans ces éléments.

Le fournisseur doit veiller à ce qu’à l’issue de chaque intervention à distance, les données résiduelles (fichiers temporaires ou zones de mémoire vive) en provenance du SIS soient effacées de la plateforme.

Toute intervention de télémaintenance doit faire l’objet d’une communication transmise à la DSI dans les meilleurs délais, par exemple sous forme d’un rapport mensuel.

Le centre hospitalier met à disposition un portail SSL pour toute opération à distance. Celui-ci doit être privilégié :

* Le point d’accès distant est protégé contre les attaques logiques en provenance des réseaux et son contournement en vue d’accéder au réseau du système d’information ne doit pas être possible dans la pratique.
* Des contrôles de conformité et d’intégrité sont mis en place à l’aide de règles définies par le service informatique (version à jour de l’anti-virus, des correctifs du système d’exploitation, du navigateur, du pare-feu….) pour vérifier les postes informatiques de la société lors des accès en télémaintenance.
* Tout accès distant est tracé et conservé.
* Les échanges entre la plateforme d’intervention et le point d’accès distant au système d’information sont protégés par des fonctions de chiffrement et d’authentification mutuelle. Ces fonctions sont de préférence conformes au Référentiel Général de Sécurité (RGS).

Si le point d’accès distant n’est pas la solution adoptée, il appartient au service informatique de décider sur recommandation du fournisseur de la solution et du protocole utilisés pour l’échange entre les équipements objets de l’intervention et la plateforme. Dans ce cas les échanges doivent être protégés de bout en bout par des fonctions de chiffrement et d’authentification mutuelle ; ces fonctions étant de préférence conformes au Référentiel Général de Sécurité (RGS).

Chaque équipement objet d’une télésurveillance ou d’une télémaintenance dispose d’un compte réservé à cette fin et dont les paramètres d’identification et d’authentification sont différents de ceux de tout autre équipement.

1. Dispositions particulières pour la sécurité du système d’information

Ce paragraphe concerne les dispositions mises en œuvre par la DSI sur le Système d’Information de l’établissement.

L’utilisation de compte générique n’est pas autorisée dans le cadre de prestation. Les accès sont donc nominatifs pour chaque intervenant de la société identifié lors des différentes demandes. Leur validité est définie selon la durée du contrat et soumis à autorisation d’un responsable de l’équipe de rattachement au sein de l’établissement.

La connexion directe du prestataire sur des équipements contenant des applications ou des informations à caractère personnel doit être évitée.

Dans la mesure du possible, le prestataire doit demander une autorisation d’accès au service informatique. En cas d’urgence, il informe l’établissement de chaque opération de maintenance dont il prend l’initiative (natures des opérations, noms des intervenants). En fin d’intervention ou en cas de complications, il tient informé la DSI des difficultés et solutions mises en œuvre.

L’utilisation de matériels ou logiciel sur les postes de travail ou les serveurs de l’établissement sont soumis à qualification de la part de la DSI selon les procédures mises en place.

ANNEXE 1 : ENGAGEMENT PERSONNEL DU FOURNISSEUR / PRESTATAIRE

Je soussigné, .................................................................................................................. , déclare avoir pris connaissance et compris la « Charte des Prestataires intervenant sur le Système d'Information » du CHU-Hôpitaux de Rouen et m'engage à la respecter.

Fait à .................................................... le ...................................

Signature :