



Charte définissant les règles de sécurité applicables aux prestataires accédant au Système d'Information du CHU de Rennes



Emeric GUILLOU	Correspondant Sécurité du SI	03/01/2018	VALIDE
Frédéric ALLIAUME	RSSI adjoint	03/01/2018	VALIDE
Christine PICHON	RSSI	03/01/2018	VALIDE
Véronique ANATOLE-TOUZET	Directrice Générale	04/04/2018	VALIDE

MISE EN ŒUVRE ET REVISION DU DOCUMENT

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) de l'établissement est en charge de la diffusion, de la mise à jour et de la révision du document.

HISTORIQUE DU DOCUMENT

Version	Date	Nom	Actions
0.2	07/02/2017	Wavestone	Livraison initiale
0.3	14/02/2017	Wavestone	Mise à jour suite revue du 14/02/2017
1.0	13/03/2017	Emeric Guillou	Relecture des modifications et approbation
1.0	16/03/2017	Emeric Guillou	Relecture des modifications et approbation



Sommaire

1. Préambule.....	4
2. Règles de sécurité à respecter	4
2.1 Confidentialité des données	4
2.2 Protection des accès aux SI.....	5
2.3 Protection des comptes et droits d'accès.....	6
2.4 Déclaration des vulnérabilités et incidents	6
2.5 Traçabilité et contrôle.....	6
2.6 Sanctions.....	7
3. Engagement du prestataire.....	8



1. PREAMBULE

Le Système d'Information constitue une ressource stratégique indispensable pour le CHU de Rennes dans la conduite de son activité. Ce Système d'Information étant exposé à de nombreux risques en termes de sécurité (accidents, erreurs, malveillances, etc.), une Politique de Sécurité du Système d'Information (PSSI) a été élaborée pour définir les principes et règles de sécurité, et préciser les rôles et responsabilités de chacun. La présente charte s'inscrit dans le cadre de la PSSI. Elle est de ce fait un document de référence pour l'ensemble des entités du CHU de Rennes.

Dans cet objectif, la présente charte, relative à l'accès et à l'utilisation des ressources du Système d'Information du CHU de Rennes, précise les règles et précautions que les prestataires doivent respecter afin de garantir un usage fiable et sécurisé des ressources du Système d'Information.

Elle s'applique à tous les éléments du Système d'Information mis à la disposition des prestataires par le CHU (matériels fixes ou nomades, logiciels, systèmes de communication en interne ou en externe, etc.), ainsi qu'aux données stockées ou véhiculées par ces éléments.

Elle s'adresse à tout prestataire autorisé à accéder, traiter ou utiliser des ressources du Système d'Information du CHU de Rennes dans le cadre de son activité professionnelle.

Cette charte complète le contrat signé avec le prestataire mais ne s'y substitue pas. Elle n'a pas pour objet de couvrir de façon exhaustive tous les cas de figure possibles, mais plutôt de fixer les principes généraux d'utilisation : c'est donc à l'esprit de ces principes que le prestataire devra se conformer dans des situations non envisagées.

En signant cette charte, le prestataire reconnaît en avoir pris connaissance et s'engage librement à en appliquer strictement le contenu.

2. REGLES DE SECURITE A RESPECTER

Chaque prestataire s'engage à respecter les règles de sécurité définies par le CHU, incluant les règles dictées dans la Charte informatique et relatives à l'usage du Système d'Information de l'établissement (poste de travail, internet, messagerie, etc.), ainsi que la Charte d'administration du SI lorsqu'applicable dans le cadre de sa mission.

2.1 Confidentialité des données

Le prestataire s'engage à garantir en toutes circonstances la confidentialité des informations du CHU.

Le prestataire s'engage à ne prendre connaissance des informations du CHU ou à n'y donner accès que dans le cadre de ses attributions ou sur demande d'une personne habilitée du CHU de Rennes.

Le prestataire veille à ne pas prendre connaissance des données de santé ou des données personnelles d'utilisateurs (messagerie, fichiers sur le poste de travail, identifiant et mot de



passee, etc.) et à n'autoriser personne à y accéder, sauf demande formelle par une personne habilitée.

Il veille à ne pas utiliser les documents et informations obtenus ou produits à d'autres fins que celles prévues au contrat et à ne divulguer aucune information sensible sans autorisation du CHU, et ce y compris au sein de sa société.

Le prestataire s'engage à ne prendre aucune copie des documents, données et supports d'informations qui lui sont confiés ou auxquels il a accès, à l'exception de celles nécessaires à l'exécution de la prestation prévue au contrat ou de celles explicitement autorisées par le RSSI du CHU de Rennes.

Il s'assure de prendre toutes les mesures nécessaires pour assurer la confidentialité des informations qui lui sont confiées pendant la durée du contrat.

À la fin de contrat ou de son intervention, il procède à la destruction de tous les documents physiques ou numériques contenant des données du CHU de Rennes.

2.2 Protection des accès aux SI

Le prestataire s'engage à utiliser les seuls moyens d'accès au SI mis à disposition ou validés par le CHU, qu'il s'agisse d'accès depuis le site du CHU ou à distance. Il respecte les procédures et règles communiquées par le CHU pour accéder au SI.

Il veille à ne pas outrepasser ni tenter de contourner les mesures de sécurité et le contrôle d'accès en place, pour quelque raison que ce soit.

Le prestataire veille à ne pas connecter de matériel non fourni par le CHU sur le réseau interne du CHU de Rennes sans autorisation préalable de la DIFSI.

Lors de ses accès aux salles informatiques du CHU, le prestataire respecte les règles suivantes :

- Toute intervention dans les salles informatiques doit faire l'objet d'une validation préalable formelle du CHU ;
- Lorsque l'intervention est en dehors des heures ouvrées, le prestataire doit se présenter au poste de Sécurité ;
- L'intervention sera, dans la mesure du possible, encadrée par une personne habilitée du CHU ;
- Sur demande du CHU, le prestataire doit fournir un rapport d'intervention détaillant les opérations réalisées, exhaustif et officiel.

Lors de ses accès à distance au SI du CHU, le prestataire respecte les règles suivantes :

- Toute intervention sur le SI doit se faire dans le strict respect des règles définies par le CHU ; Sur demande du CHU, le prestataire doit fournir au CHU un rapport d'intervention détaillant les opérations réalisées, exhaustif et officiel.



2.3 Protection des comptes et droits d'accès

Le prestataire s'assure de la protection des comptes et droits d'accès qui lui sont confiés. Il veille notamment à la protection des identifiants et authentifiants qui lui sont confiés.

Il ne les utilise que pour les activités et besoins directement liés aux tâches dont il a la charge. En particulier, il veille à ne pas abuser de ses privilèges, et limite ses actions aux ressources informatiques auxquelles il a accès, dans le respect de la finalité de sa mission.

En particulier, il ne modifie les configurations et les droits d'accès que dans le cadre des procédures définies, lorsqu'elles existent.

Il veille à ne pas prendre de consignes d'une personne non autorisée et à escalader auprès du pilote de la mission du CHU de Rennes toute requête lui paraissant contraire aux règles de sécurité du CHU de Rennes ou à la législation en vigueur.

Pour les accès aux ressources du SI du CHU de Rennes, il utilise des mots de passe robustes respectant les règles définies dans la PSSI :

- Le mot de passe doit contenir au moins 8 caractères ;
- Le mot de passe doit contenir au moins 3 des 4 types de caractères suivants :
 - o Lettres minuscules,
 - o Lettres majuscules,
 - o Chiffres,
 - o Caractères spéciaux ;
- Le mot de passe doit être difficile à deviner ;
- Le mot de passe ne doit pas être un mot du dictionnaire ni un élément en rapport avec la vie courante (prénom du conjoint ou des enfants, date de naissance, de mariage, etc.) ;
- Tout nouveau mot de passe doit être différent des 3 précédents mots de passe.

Le prestataire s'engage à ne pas noter le mot de passe ou tout autre code d'authentification dans un endroit non sûr (ex. post-it à proximité du poste, en clair dans un fichier).

Il s'engage par ailleurs à verrouiller sa session lorsqu'il s'absente de son poste et à ne pas laisser le poste accessible sans surveillance.

2.4 Déclaration des vulnérabilités et incidents

Le prestataire s'engage à remonter sans délai à son correspondant du CHU toute vulnérabilité et tout incident de sécurité qu'il constate ou suspecte, incluant la perte ou le vol de supports informatiques contenant des données du CHU, ou bien la compromission d'un compte d'accès au SI de l'établissement.

2.5 Traçabilité et contrôle

Le CHU de Rennes se réserve le droit de vérifier, par tout moyen, le bon usage des ressources informatiques et le respect des règles édictées par la présente charte.

L'utilisation des ressources informatiques de l'établissement génère des traces informatiques pouvant contenir des données à caractère personnel des utilisateurs, telles l'adresse IP ou



l'identifiant du poste de travail, le login de l'utilisateur, les dates et heures des actions, les ressources accédées et/ou les actions réalisées.

Ces traces peuvent faire l'objet de traitements par l'établissement à des fins statistiques, de maintenance des équipements, de contrôle du respect des règles de sécurité, de respect des droits des patients, de protection du SI et des informations qu'il contient, ou d'enquêtes en cas d'incident ou de suspicion d'incident technique ou de sécurité.

Les traitements réalisés sur ces données respectent les exigences légales et réglementaires.

2.6 Sanctions

En cas de violation manifeste et/ou répétée des règles édictées dans ce document, des lois, des règlements, ou de la déontologie, le prestataire engage sa propre responsabilité et s'expose à des sanctions pouvant aller jusqu'à l'exclusion de l'établissement ou la rupture du contrat.

Selon la gravité des faits constatés, l'établissement se réserve par ailleurs le droit d'engager des poursuites à l'encontre de l'utilisateur.



3. ENGAGEMENT DU PRESTATAIRE

Je soussigné,, employé de la société, déclare avoir pris connaissance et compris la « Charte prestataires » du CHU de Rennes et m'engage à ce qu'elle soit respectée dans la cadre des activités de la mission qui lui est confiée.

- Objectifs et activités de la mission :
- Périmètre technique (si applicable) :
- Dates et plages horaires d'intervention (si applicable) :
- Correspondant(s) CHU de Rennes :

Fait à le

Signature