



**GROUPEMENT
HOSPITALIER
DE TERRITOIRE**
LOIRE ATLANTIQUE

DIRECTION DES SERVICES NUMERIQUES

**Charte de télémaintenance
pour les fournisseurs du GHT44**

Auteur : Cédric CARTAU
Approbateur : Eric MALEVIALLE
Statut : Validé
Classification : PUBLIC

NOTES DE REVISION

DATE	AUTEUR	
06/03/2026	CWC	Version initiale avant traçabilité des modifications

Table des matières

1	PREAMBULE	4
2	TELEMAINTENANCE	4
3	CINEMATIQUE DE CONNEXION.....	5
4	ASPECTS JURIDIQUES	5
4.1	Responsabilité	5
4.2	Respect des lois en vigueur	6
4.3	Intitulé des clauses	6
4.4	Invalidité d'une clause	6
4.5	Réglementation NIS 2	6
4.6	Exceptions	6
5	SIGNATURE DU FOURNISSEUR.....	7

1 PREAMBULE

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 (SI) du GHT44, ci-après nommé Personne Publique (PP).

Elle a pour objet de définir les conditions et modalités que le Fournisseur (sous marché ou agissant dans le cadre d'une sous-traitance pour le compte du Titulaire du marché) s'engage à respecter dans le contexte d'un accès au SI de la PP par de la télémaintenance afin d'assurer la sécurité des SI (SSI) de la PP 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).

Cette charte et les règles qu'elle contient ont été établies en tenant compte de la Politique de Sécurité de la PP et sous l'autorité du Responsable de la Sécurité des Systèmes d'Information. Elle fait partie du référentiel de sécurité de la PP approuvé par la Direction Générale de l'établissement. Elle complète tout Marché liant le fournisseur à la PP. Son respect constitue une obligation essentielle à la charge du fournisseur.

2 TELEMaintenance

Aucun accès par modem n'est autorisé : tous les accès au système d'information de la PP depuis l'extérieur devront passer par les équipements de sécurité validés par la DSN : VPN, Firewall, bastion d'administration etc.

En cas de télémaintenance permettant l'accès à distance aux ressources du SI de la PP, le Fournisseur devra mettre en œuvre tous les moyens organisationnels pour :

- obtenir l'accord préalable de la PP 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 DSN. Il en va de même pour les environnements d'intégration ;
- prendre toutes dispositions afin de permettre à la PP d'identifier la provenance de chaque intervention extérieure ;
- prendre les dispositions en interne afin de tracer nominativement les membres de son personnel qui accèdent en télémaintenance ; il est possible d'utiliser des comptes génériques sous réserve de la mise en place d'un fonctionnement de type « main courante » avec trace écrite informatisée, à la charge du fournisseur ; en cas d'impossibilité, la responsabilité juridique est portée par le responsable administratif du Fournisseur ;
- 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) dans un délai de 72h maximum ;
- cet accès est exceptionnel, et délivré par la PP pour une durée maximale de 6 mois, éventuellement renouvelable en fonction du contexte ;

Pour ce qui concerne l'accès aux données de la PP :

- 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. Tout accès en direct à un serveur de production doit avoir été validée au préalable par la DSN par écrit (mail de confirmation par exemple). Il peut d'agir d'accès justifiés par l'urgence de l'intervention technique. Tout manquement à cette règle engage la responsabilité juridique du fournisseur.
- Lorsque le marché inclut l'accès par le fournisseur aux postes de travail des agents du CHU :
 - o en aucun cas cet accès ne constitue un droit de visualiser des données d'accès restreint (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 ;

Les dispositions techniques suivantes devront avoir été mises en place par le Titulaire (les accès distants pour télémaintenance ne respectant pas ces dispositions seront supprimés aux seuls frais directs et indirects du Titulaire de l'accès) :

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

Enfin pour les accès en télémaintenance :

- fermeture des accès par défaut (le compte fournisseur existe mais reste bloqué par défaut en attendant un déblocage manuel nécessitant une intervention humaine d'un agent de la DSN) ;
- déblocage d'un accès uniquement sur demande écrite et motivée, provenant d'une adresse mail référencée sur la fiche fournisseur ;
- rappel par les équipes d'exploitation d'un numéro (également référencé) demandant un élément de confirmation (par exemple un code ou numéro dédié à chaque client déterminé à la mise en place du canal de télémaintenance) ; une fois seulement le compte activé, connexion possible ;
- re-verrouillage du compte après l'intervention, soit manuellement soit par script automatisé ;
- rupture de flux, seule la prise de main à distance sur un terminal est possible, pas d'accès VPN direct ;
- filtrage sur une adresse IP fixe, fournie par le prestataire au moment de la mise en place du contrat ; cela signifie entre autres que les agents du fournisseur devront repasser par l'IP de sortie de leur employeur pour les accès distants en télémaintenance, y compris quand eux-mêmes se trouvent en télétravail ;
- géoblocking généralisé aux IP européennes ; il appartiendra au client de mettre en place, dans son infrastructure et à ses frais, des IP européennes de sortie avec des backup (le géoblocking produit des faux positifs) ;
- durée d'un compte fournisseur strictement limité à la durée du marché ;
- obligation contractuelle du fournisseur de signaler tout changement, tout incident ;
- MFA à mettre en place, par le fournisseur sur son propre SI avec obligation contractuelle, pour sécuriser les accès télémaintenance sortants ;
- fin des accès LAN to LAN ;
- séparation entre les accès sortant (pour télé-supervision d'équipements) et des accès entrants ;
- obligation réglementaire du fournisseur à former ses agents, y compris ses prestataires en sous-traitance, avec preuve de formation, à renouveler à minima tous les 3 ans ;
- le fournisseur est responsable, civilement et pénalement en cas de manquement à ses obligations réglementaires (identifiants dans la nature, MFA pas mis en place, formations pas suivies, etc.).
- les exceptions sont formellement validées par le RSSI, tracées, limitées dans le temps et auditable.

3 CINEMATIQUE DE CONNEXION

La connexion est réalisée sur un accès VPN de type IPSec ou SSL, et ensuite le fournisseur se connecte à une machine de rebond sur le LAN avec un compte AD dédié, qui lui permet enfin de prendre la main sur l'équipement en télémaintenance.

4 ASPECTS JURIDIQUES

4.1 Responsabilité

Conformément à la loi, le Fournisseur est responsable de tous les dommages ou préjudices 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, des sanctions civiles (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) pourront être prononcées par les juges.

4.2 Respect des lois en vigueur

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 réglementation relative à la protection des traitements de données nominatives, qui fait l'objet d'un document annexé à part (RGPD, en vigueur à partir du 25 mai 2018) ;
- 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 ;
- les dispositions relatives au Référentiel Général de Sécurité ;

La présente charte est de plus conforme aux normes en vigueur :

- la norme ISO 27 000 ;
- les bonnes pratiques recommandées par l'ANSSI, et en particulier le guide d'hygiène ;
- les bonnes pratiques recommandées par l'ASIP ;

4.3 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.

4.4 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.

4.5 Réglementation NIS 2

Le fournisseur indique s'il est soumis à NIS2, et le cas échéant s'il est Entité Essentielle ou Entité Importante. Le fournisseur a bien pris conscience, le cas échéant, des obligations afférentes à cette directive, notamment concernant les obligations d'alerte et les amendes en cas de non-respect.

Egalement, les manquements aux obligations NIS2 de la PP consécutives au non-respect des règles d'hygiène numérique de base par le Fournisseur engage la responsabilité juridique du Fournisseur.

4.6 Exceptions

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

5 SIGNATURE DU FOURNISSEUR

Je, soussigné

Représentant de la société

Déclare accepter sans réserve les conditions du présent document.

Fait à le :

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