



GROUPEMENT
HOSPITALIER
DE TERRITOIRE
LOIRE ATLANTIQUE

DIRECTION DES SERVICES NUMERIQUES

**Charte d'accès au Système d'information
du GHT44
pour les fournisseurs du GHT44**

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

NOTES DE REVISION

DATE	AUTEUR	
20/10/2022	CWC	Version initiale avant traçabilité des modifications
19/02/2024	CWC	Rajout des contraintes réglementaires NIS2

Table des matières

1	PREAMBULE	4
1.1	Objectifs	4
1.2	Cycle de vie du document	4
2	ORGANISATION DE LA SECURITE ET DE LA CONFORMITE	4
2.1	Organisation chez la Personne Publique	4
2.2	Organisation chez le Fournisseur	5
2.3	Pilotage de la sécurité projet	5
3	CLASSIFICATION DES INFORMATIONS.....	5
3.1	Généralités	5
3.2	Cas particulier des données médicales	6
4	SECURITE LIEE AUX RESSOURCES HUMAINES.....	6
5	SECURITE DES ACTIFS.....	6
6	ACCES PHYSIQUES	6
6.1	Accès physiques aux locaux.....	6
6.2	Connexion du matériel du Fournisseur sur le réseau	7
7	ACCES LOGIQUES.....	8
7.1	Généralités	8
7.2	Sécurité des accès logiques	8
7.3	Protection contre les logiciels malveillants	9
8	TELEMAINTENANCE	9
8.1	Généralités	9
8.2	Connexion depuis l'extérieur	9
9	SECURITE LIEE A L'EXPLOITATION.....	11
9.1	Généralités	11
9.2	Engagements du Fournisseur	11
9.3	Protection antivirale	11
9.4	Mise à jour des patches de sécurité.....	11
9.5	Copies des bases de données du CHU	12
9.6	Chiffrement des échanges	12
9.7	Alertes de sécurité.....	12
10	GESTION DES INCIDENTS.....	12
11	AUDITS, TRACABILITES ET CONTROLES	12
11.1	Généralités	12
11.2	Traçabilité des accès	12
12	ASPECTS JURIDIQUES	13
12.1	Responsabilité	13
12.2	Respect des lois en vigueur	13
12.3	Intitulé des clauses	13
12.4	Invalidité d'une clause	13
12.5	Exceptions	13
13	GLOSSAIRE	14
14	SIGNATURE DU FOURNISSEUR.....	14

1 PREAMBULE

1.1 Objectifs

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 GH4TT, ci-après nommé Personne Publique (PP).

Elle a pour objet de définir les conditions et modalités que le fournisseur s'engage à respecter 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.

1.1.1 Portée et effet

Cette charte s'applique à tout marché pour lequel le fournisseur doit avoir accès à tout ou partie du Système d'Information de la PP. Le fournisseur doit la signer et se conformer à ses dispositions.

Elle s'applique à tous les personnels du fournisseur ainsi qu'aux personnels d'entreprises sous-traitantes ayant contracté avec le Fournisseur pour la prestation objet du marché.

Elle est annexée au Cahier des Clauses Techniques Particulières.

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 de la PP, tout fournisseur est soumis à la Charte Utilisateur du Système d'Information. La présente Charte Fournisseurs décrit les dispositions additionnelles spécifiques aux fournisseurs vis-à-vis du Système d'Information de la PP.

Sauf mention contraire, le fournisseur est soumis à une obligation de moyen, étant entendu que la charge de la preuve lui incombe.

1.2 Cycle de vie du document

Le présent document évolue en fonction de la réglementation et des évolutions techniques, ainsi que des remarques qui sont remontées par les équipes de la DSN.

Ce cycle de vie s'inscrit dans un processus global d'amélioration continue de type ISO 27001.

2 ORGANISATION DE LA SECURITE ET DE LA CONFORMITE

2.1 Organisation chez la Personne Publique

La SSI est portée par le RSSI.

La conformité RGPD est portée par le DPO.

Toutes les questions relatives à ces deux domaines doivent leur être adressées, toute exception aux règles en vigueur doit faire l'objet d'un accord formel de leur part.

2.2 Organisation chez le Fournisseur

Le Fournisseur doit disposer d'une politique SSI sur laquelle il s'appuie concernant le projet. Cette politique doit être communiquée sur demande.

Le Fournisseur doit mettre à disposition de la PP un interlocuteur unique concernant le volet SSI.

Pour le volet RGPD et conformément à la législation, le Fournisseur doit communiquer le nom de son DPO.

Selon la complexité du projet, le Fournisseur pourra disposer d'une équipe dédiée à ces questions, tout en respectant le principe du point d'entrée unique.

2.3 Pilotage de la sécurité projet

Selon la nature du projet, une instance spécifique SSI et / ou RGPD pourra être mis en place entre les parties.

3 CLASSIFICATION DES INFORMATIONS

3.1 Généralités

L'ensemble des informations et des documents fournis par la PP, quel que soit leur support, reste la propriété exclusive, pleine et entière de la PP. Le fournisseur devra en assurer la protection et respecter la non-divulgaration 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 de la PP 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 restreint l'ensemble des informations, documents et toute autre donnée qu'il reçoit de la PP, 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 Système d'Information de la PP, ainsi que toutes 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 des agents sous sa responsabilité toutes les mesures nécessaires pour qu'il respecte le secret et la confidentialité de toutes les informations et de tous les documents appartenant à la PP.

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 à la PP. 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 la PP, à l'exception de celles nécessaires à l'exécution de sa mission sous réserve d'avoir obtenu préalablement et par écrit l'accord exprès de la PP ;
- 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 à la PP ou, à défaut, procéder à la destruction sécurisée de chacun des supports et de chacune des informations non restitués ; à ce titre la PP 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 la PP ou leurs résultats. Le traitement doit être proportionné et conforme à la finalité prévue dans le Marché signé avec la PP, à la présente charte et les règles générales relatives à la sécurité du Système d'information de la PP.

Le Fournisseur s'interdit l'utilisation des Ressources informatiques mises à sa disposition par la PP à des fins autres que celles figurant dans le Marché.

3.2 Cas particulier des 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 validé par les pouvoirs publics.

La PP 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 de la PP.

4 SECURITE LIEE AUX RESSOURCES HUMAINES

Le Fournisseur garantit que ses personnels ont été sensibilisés à la SSI, conformément aux bonnes pratiques.

Le Fournisseur fait signer par ses employés un engagement à respecter les bonnes pratiques de SSI : confidentialité, respect des normes etc.

En cas de non-respect des bonnes pratiques de SSI par les employés du Fournisseur, c'est la responsabilité civile ou pénale du Fournisseur au titre de personne morale qui est engagée. Il appartient au Fournisseur de tracer nominativement les actions effectuées par ses employés, et en cas de faute personnelle détachable du service de la part d'un ou plusieurs de ses employés, la charge de la preuve incombe au Fournisseur.

5 SECURITE DES ACTIFS

Le Fournisseur tient à jour un inventaire exhaustif de ses actifs utilisés pour le projet. Cet inventaire est communicable sur simple demande.

Le Fournisseur applique les bonnes pratiques de sécurisation de ses actifs : classification, protection antivirale, chiffrement etc. (liste non exhaustive). Le Fournisseur est libre de faire auditer cette gestion de ses actifs.

Le Fournisseur veille en particulier à la destruction des informations qui lui ont été confiées à la fin du projet, dans le respect de la réglementation en vigueur. Cette destruction concerne à la fois les informations et les supports physiques de stockage.

6 ACCES PHYSIQUES

6.1 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 la PP. 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 la PP dans les locaux de la PP ;
- respecter les systèmes de sécurité physique mis en place au sein de la PP, 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 la PP 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 à la PP un descriptif précisant les dates, la nature des opérations à effectuer et les noms des intervenants, ainsi que les conditions de bon déroulement de la prestation (par exemple, nécessité pour les agents de la PP de préparer des documents, logiciels ou matériels).

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.

Seul le Personnel affecté aux missions définies dans le Marché signé avec la PP pourra avoir accès aux clés, codes, matériels ou locaux utilisés pour assurer la protection physique des informations et Ressources informatiques appartenant à la PP.

Chaque membre du personnel du Fournisseur 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. La PP 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, la PP 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. La PP s'engage à respecter la législation relative aux traitements de données à caractère personnel mis en place à cette fin.

6.2 Connexion du matériel du Fournisseur sur le réseau

Dans la majorité des cas, l'utilisation de matériels informatiques fournis par la PP 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 de la PP, cette connexion est possible aux conditions suivantes :

- respect de la Charte d'Utilisation du Système d'Information ;
- respect des différents Politiques Techniques de Sécurité ;
- intégration du matériel au domaine Active Directory s'il s'agit d'un OS de type Windows ;
- présence d'un antivirus à jour et à même de récupérer au moins 1 fois toutes les 24h les dernières signatures antivirales ; l'antivirus maintenu par la DSN est TREND : tout usage d'autre antivirus doit être validé par la DSN ;
- présence d'un Système d'Exploitation maintenu par son éditeur et dont les patches de sécurité sont toujours diffusés : Windows, Linux etc. et à même de récupérer au moins 1 fois par semaine les derniers patches de sécurité ;
- respect des contraintes d'adressage MAC et IP de la DSN ;
- le Fournisseur devra démontrer que son matériel ne présente aucun risque de compromission ou d'infection du réseau informatique de la PP ;

- cette connexion ne doit en aucune manière avoir un impact sur les performances, la disponibilité, l'intégrité et la confidentialité du Système d'Information de la PP ;
- le matériel doit se connecter au réseau de la PP par les prises habituelles (Switch, prises RJ45 etc.) ; les connexions à l'aide de modem sont interdites ;

Tout équipement qui ne respecte pas ces principes de base ne pourra être connecté que sur un VLAN isolé derrière un pare-feu interne. Dans ce cas, le Fournisseur devra communiquer la liste des IP et des ports de connexion pour l'interface entre son système et le reste du LAN, sous sa seule responsabilité.

Le Fournisseur s'engage à ne connecter aucun matériel informatique sans l'accord explicite et écrit de la DSN ou du RSSI de la PP.

7 ACCES LOGIQUES

7.1 Généralités

Tout accès logique au Système d'Information de la PP nécessite au préalable :

- L'attribution par la DSN d'un compte utilisateur Active Directory, actif pour le temps exclusif de la prestation et / ou de la connexion ;
- Dans les cas exigés par la réglementation, 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 collectifs en fonction du domaine, des besoins et de la législation.

7.2 Sécurité des accès logiques

Il appartient au Fournisseur de s'assurer de la bonne utilisation des comptes utilisateurs qui lui ont été fournis, 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 départ éventuels de personnels chez le Fournisseur ; 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 ;
- assurer de façon générale la protection contre tout accès non autorisé par tous les moyens adéquats (protection périmétrique, protection physique etc.) ;

Le Fournisseur et son Personnel s'engagent à :

- faire respecter la protection, la non-divulcation 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 ;
- 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 Systèmes d'Information de la PP, 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 de la PP ;

Le Personnel du Fournisseur devra avertir la DSN 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 consiste à prévenir par tout moyen et dans les plus brefs délais la DSN ou le RSSI, qui s'attachera à isoler le dysfonctionnement.

7.3 Protection contre les logiciels malveillants

Ce paragraphe fait référence aux virus, spyware, 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 de la PP définie dans la politique Technique de Sécurité Anti-Malware.

Les machines introduites sur le réseau devront avoir une protection antivirale (identique à celle de la PP) à jour (dernière version disponible de la base de signatures) 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 DSN.

De même, tous les supports d'informations (disquettes, clés USB, CD-ROM etc.) devront avoir été balayés, en présence d'un agent de la DSN, par un antivirus à jour, chaque fois qu'ils doivent être utilisés sur les matériels de la PP. Le Fournisseur s'engage à procéder de même pour l'utilisation de tels supports sur son propre matériel.

Lorsque le Fournisseur intervient sur site, la PP se réserve le droit d'installer soi-même 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.

8 TELEMANTENANCE

8.1 Généralités

La télémaintenance est nécessaire au bon maintien en condition opérationnelle de beaucoup d'équipements utilisés par la PP.

Elle se divise en 2 cas d'utilisation en fonction du type de contrat :

- cas 1 : le fournisseur a positionné sur le LAN de la PP 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 ;
- cas 2 : le fournisseur se connecte, depuis l'extérieur de la PP, à un équipement situé sur le LAN ou dans la DMZ de la PP ; il s'agit de télémaintenance à proprement parlé ;

Il appartient au Fournisseur de tester au moins tous les 6 mois son accès en télémaintenance : par mesure de sécurité, les accès non utilisés depuis plus de 6 mois sont verrouillés et la réouverture doit se faire en appelant la DSN.

Les accès fournis par la PP sont nominatifs ou génériques selon les cas, et sont sous la seule responsabilité du Fournisseur. En particulier, les mots de passe sont transmis par la PP par canal sécurisé. Le Fournisseur s'engage à communiquer sans délai tout incident compromettant un accès.

8.2 Connexion vers l'extérieur

Le canal ouvert est unidirectionnel : il est strictement interdit de l'utiliser pour effectuer des accès entrants, ces derniers doivent passer par les équipements d'interconnexion décrits ci-après.

Seuls les protocoles standards et sécurisés sont autorisés : SMTPS, HTTPS, etc.
Toutes les connexions doivent être profitables.

8.3 Connexion depuis l'extérieur

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.

De plus :

- Les accès en télémaintenance peuvent devoir passer par un point d'accès unique fourni et qualifié par la DSN : VPN Ipsec, bastion d'administration, etc. ;
- il est nécessaire de tracer nominativement les personnes des sociétés extérieures 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 ;

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 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 ;
- 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 DSN, 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. Tout accès en direct à un serveur de production doit avoir été validé 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 :

- cet accès est exceptionnel, et délivré par la PP pour une durée maximale de 6 mois, éventuellement renouvelable en fonction du contexte ;
- tout usage de cet accès doit faire l'objet d'une fiche d'intervention, rédigée par le fournisseur et transmise sous 24h au responsable applicatif DSN ;
- 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 ;

Enfin et d'ici le 31/12/2023, les dispositions suivantes devront avoir été mises en place. Les accès distants pour télémaintenance ne respectant pas ces dispositions seront supprimés aux seuls frais directs et indirects du Titulaire de l'accès :

- 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.

9 CINEMATIQUE DE CONNEXION

Les cinématiques de connexion autorisées sont décrites en annexe.

10 SECURITE LIEE A L'EXPLOITATION

10.1 Généralités

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

10.2 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 de la PP : 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 de la PP 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 de la PP afin de procéder à une démonstration (par exemple de la nouvelle version d'un progiciel déjà détenu par la PP) directement dans un service utilisateur et sans passer par le point de contact unique qui est la DSN, qui devra avoir explicitement et par écrit autorisé une telle utilisation.

10.3 Protection antivirale

Compte tenu du risque majeur d'infection virale informatique, le Fournisseur prend toutes les précautions pour protéger ses actifs : antivirus résidents, scans réguliers, pas d'utilisation de clé USB, transfert d'information qui utilise des canaux sains (passage par des proxy de désinfection) etc.

10.4 Mise à jour des patches de sécurité

Les patches de sécurité sont maintenus et déployés par la partie qui a fourni les logiciels sous sa responsabilité.

10.5 Chiffrement des échanges

Par défaut, tous les échanges de données entre le Fournisseur et la PP utilisent le chiffrement : chiffrement de la messagerie, utilisation de plateformes sécurisées pour les échanges, etc.

11 GESTION DES INCIDENTS

Le Fournisseur doit formaliser un processus de gestion des incidents.

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

12 AUDITS, TRACABILITES ET CONTROLES

12.1 Généralités

Tout accès au SI de la PP est tracé, conformément aux lois informatiques et Liberté.
Les traces sont conservées 1 an.

12.2 Traçabilité des accès

Il appartient au Fournisseur, dans le cas de l'attribution d'un compte utilisateur générique (c'est-à-dire affecté au Fournisseur et non pas nominativement à un ou plusieurs employés) de gérer la traçabilité des accès.

La PP doit, sur simple demande, pouvoir disposer de l'historique nominatif de l'utilisation de cet accès générique, s'entend quel employé du Fournisseur a utilisé cet accès, à quelles dates et heures, pour quelle durée et pour quelle action.

13 POINTS ADDITIONNELS

13.1 Alertes de sécurité

Les alertes de sécurité sont signalées par le fournisseur à exploitation@chu-nantes.fr

13.2 Copies des bases de données de la PP

Qu'il s'agisse de maintenance technique ou autre, toute copie de données de la PP est soumise à stricte autorisation de la DSN et du RSSI.

Un fournisseur qui copierait des données du GHT44 sans autorisation formelle s'exposerait à des poursuites immédiates.

14 ASPECTS JURIDIQUES

14.1 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.

14.2 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 ;

14.3 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.

14.4 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.

14.5 Exceptions

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

14.6 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.

15 GLOSSAIRE

« 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 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...), 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 GHT44. 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.

« DSN »

Direction des Systèmes d'Informations et de Télécommunication du CHU de NANTES.

« RSSI »

Responsable Sécurité des Systèmes d'Information du CHU de NANTES.

16 SIGNATURE DU FOURNISSEUR

Je, soussigné

Représentant de la société

Déclare accepter sans réserve les conditions du présent document, et avoir pris connaissance des obligations réglementaires (RGPD, directive NIS2, etc.)

Fait à

le :

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