

1. Objet	2. Domaine d'application
<p>La présente charte décrit les règles de sécurité applicables dans le cadre des interventions de fournisseurs ou prestataires utilisant les moyens informatiques ou de télécommunication d'un Etablissement du Groupement Hospitalier Brocéliande Atlantique ou bénéficiant d'un accès à distance aux Systèmes d'information, directement ou à partir du Réseau dudit Etablissement.</p>	<p>Sécurité des Systèmes d'Information.</p>
3. Définition et abréviations	4. Responsabilités
<p>ANSSI : Agence Nationale pour la Sécurité des Systèmes d'Information</p> <p>SI : Système d'Information</p> <p>Etablissement : désigne un Etablissement partie du Groupement Hospitalier Brocéliande Atlantique ou l'EHPAD La Rose des Vents de Quiberon.</p>	<p>Direction, Direction des établissements parties du GHT, RSSI, DSIT, DITP, Service Biomédical</p>

SOMMAIRE

ARTICLE 1. ENGAGEMENTS DU FOURNISSEUR / DU PRESTATAIRE	3
1. DISPOSITIONS ADMINISTRATIVES GENERALES	3
2. CONSIGNES DE SECURITE POUR LE PERSONNEL OU LE SOUS-TRAITANT DU FOURNISSEUR / DU PRESTATAIRE	3
3. REGLES REGISSANT LES INTERVENTIONS	4
4. ACCES PHYSIQUES SUR SITE	4
5. ACCES DISTANT AU SI	4
6. PLAN D'ASSURANCE SECURITE (PAS).....	5
ARTICLE 2. ENGAGEMENTS DE L'ETABLISSEMENT	6
ARTICLE 3. MODALITES PRATIQUES DE MISE EN ŒUVRE	7

ARTICLE 1. ENGAGEMENTS DU FOURNISSEUR / DU PRESTATAIRE

1. DISPOSITIONS ADMINISTRATIVES GENERALES

- a) Le fournisseur / le prestataire doit être une entité ou une partie d'une entité dotée de la personnalité morale de façon à pouvoir être tenu juridiquement responsable de la prestation.
- b) Le fournisseur / le prestataire doit être soumis au droit d'un Etat membre de l'Union Européenne et respecter les droits et règlements qui lui sont applicables.
- c) Le fournisseur / le prestataire est tenu de déclarer tout changement relatif à sa situation administrative.
- d) Le fournisseur / le prestataire a, en sa qualité de professionnel, un devoir de conseil vis-à-vis de l'Etablissement.
- e) Le fournisseur / le prestataire informe, dès la signature du contrat, l'Etablissement de la possibilité d'utilisation de la sous-traitance.
- f) En cas de recours à la sous-traitance, le fournisseur / le prestataire répercute les exigences qui lui sont applicables vers le sous-traitant, sous son entière responsabilité.
- g) Le fournisseur / le prestataire doit décrire l'organisation de son service pour la réalisation des prestations d'installation et ou de support informatique auprès de l'Etablissement.
- h) Le fournisseur / le prestataire doit souscrire une assurance couvrant les éventuels dommages causés à l'Etablissement et notamment au système d'information dans le cadre de sa prestation.
- i) Le fournisseur / le prestataire doit s'assurer du consentement de l'Etablissement avant toute communication d'informations obtenues ou produites dans le cadre de sa prestation.
- j) Le fournisseur / le prestataire doit disposer des licences valides des outils (matériels et logiciels) utilisés pour la réalisation de la prestation.

2. CONSIGNES DE SECURITE POUR LE PERSONNEL OU LE SOUS-TRAITANT DU FOURNISSEUR / DU PRESTATAIRE

- a) Le fournisseur / le prestataire s'engage vis-à-vis de la confidentialité des informations auxquelles son personnel ou son sous-traitant peut avoir accès. Chaque personne concernée (intervenant sur site ou à distance) signe un engagement individuel de confidentialité annexé à son contrat de travail ou à son contrat de sous-traitance.
- b) Le fournisseur / le prestataire s'engage vis-à-vis des actions que son personnel ou son sous-traitant peut effectuer. Chaque personne concernée doit avoir signé un engagement individuel de limitation de ses actions au seul besoin des interventions. Cet engagement peut être regroupé avec le précédent.
- c) A minima, le fournisseur / le prestataire 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.
- d) Le fournisseur / le prestataire doit tenir à jour l'inventaire de l'ensemble des équipements mettant en œuvre le service.
- e) Le fournisseur / le prestataire doit documenter et mettre en œuvre une procédure de mise au rebut des actifs du système d'information du service. Pour les supports de stockage, cette procédure doit au minimum inclure la procédure d'effacement sécurisé ou de destruction physique par incinération ou étiquetage.

- f) Le fournisseur / le prestataire doit s'assurer que lors de la sortie d'un actif du système d'information du service, l'actif en question ne contienne plus aucune information en clair relative au système d'information du service ou au système d'information de l'Etablissement.

3. REGLES REGISSANT LES INTERVENTIONS

Le fournisseur / le prestataire s'engage formellement à :

- a) 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 de l'Etablissement est nécessaire ;
- b) Ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- c) Ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- d) Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- e) 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 ;
- f) Et en fin de contrat procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

4. ACCES PHYSIQUES SUR SITE

Tout fournisseur / prestataire doit connaître et appliquer les politiques, procédures et standards de sécurité de l'Etablissement lorsque celui-ci intervient dans les locaux de l'Etablissement 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 ou le sous-traitant du fournisseur / du prestataire est accompagné sur site en zone sensible par un personnel habilité de la DSIT de l'Etablissement.
- Les prestations réalisées et l'éventuelle remise en état avant de quitter le site, font l'objet d'une validation formelle de la part de l'Etablissement. Le fournisseur / le prestataire s'engage à respecter les procédures et processus définis par l'Etablissement 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.

5. ACCES DISTANT AU SI

- Le fournisseur / le prestataire doit assurer la sécurité de sa plateforme d'intervention à distance, des points de vue accessibilité, protection des données et des logiciels.
- Le fournisseur / le prestataire doit restreindre les accès logiques des postes d'intervention aux seules personnes autorisées.
- Le fournisseur / le prestataire doit restreindre autant que faire se peut les accès physiques des postes d'intervention aux seules personnes autorisées.
- S'il le désire, l'Etablissement a la possibilité de faire réaliser des contrôles des dispositions de sécurité prises par le fournisseur / le prestataire pour la réalisation de sa prestation.
- Le fournisseur / le prestataire doit être en mesure de déterminer en toute circonstance l'identité de toute personne qui se connecte ou s'est connectée sur le SI de l'Etablissement et en assurer la traçabilité.

- Le fournisseur / le prestataire 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 SI 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 / du prestataire 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 SI, sous la responsabilité du fournisseur / du prestataire. Par exemple : signaler les vulnérabilités en vue d'une prise de décision commune à leur égard ;
 - la lutte contre la propagation de codes malveillants ou d'incidents de sécurité à partir de la plateforme du fournisseur / du prestataire, 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 / le prestataire doit mettre en œuvre un dispositif de gestion de configuration permettant de contrôler les accès aux composants produits ou fournis au titre de la télémaintenance des logiciels (code source, code exécutable, documentation, données de tests etc...). Il s'agit bien de tracer sur la plateforme du fournisseur / du prestataire les interventions sur les composants de télémaintenance, afin d'éviter la mise en place d'accès mal maîtrisés.
- Le fournisseur / le prestataire 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 SI soient effacées de la plateforme.
- Il est à noter que certaines interventions nécessitent plusieurs sessions de connexion sur le SI (pour des raisons d'investigation par exemple). Une intervention n'est considérée comme terminée que lorsque l'objectif de l'intervention est atteint (résolution d'un incident, mise à jour d'un composant...) ou que le responsable du SI et le fournisseur / le prestataire déclarent d'un commun accord que l'objectif n'est pas atteignable.

6. PLAN D'ASSURANCE SECURITE (PAS)

Le fournisseur / le prestataire doit établir un PAS qui décrit les dispositions de sécurité qu'il met en œuvre pour sa prestation. Ce PAS peut être un sous-ensemble du plan d'assurance qualité (PAQ). À la signature du contrat, le responsable du SI doit pouvoir indiquer s'il accepte le PAS type du fournisseur. Le PAS fait partie des documents applicables du contrat disponible via internet sur l'espace client du site du fournisseur. Le PAS traite au minimum les thèmes suivants :

- Critères de sécurité utilisés dans la désignation des personnes chargées de l'intervention, engagement de sécurité, information de ces personnes sur la sécurité de la prestation et sensibilisation ;
- Règles de protection des informations relatives au SI ou à l'intervention et détenues par le fournisseur / le prestataire (copie, diffusion, conservation, destruction, transmission) ;
- Désignation des sites d'exécution de la prestation, protection et accès physiques des locaux utilisés, séparation vis-à-vis d'autres prestations ;
- Architecture générale de la plateforme utilisée pour l'intervention à distance, cloisonnement technique vis-à-vis d'autres prestations, fonctions de sécurité activées dans la plateforme ;
- Accès logique des intervenants à la plateforme, identification et authentification, mise en veille et déconnexion automatiques, séparation des tâches, gestion des droits, traçabilité des actions ;

- Dispositions prises pour continuer à assurer les activités de la prestation à la suite d'un sinistre majeur ;
- Assurance et contrôle de la sécurité des services d'intervention fournis.

ARTICLE 2. ENGAGEMENTS DE L'ETABLISSEMENT

Les dispositions suivantes sont mises en œuvre par la DSI sur le SI de l'établissement.

- La connexion directe du fournisseur / du prestataire en télémaintenance sur des équipements contenant des applications ou des informations à caractère personnel est interdite.
- Dans la mesure du possible, un point (ou passerelle) d'accès distant est mis en place pour accéder aux équipements objets de l'intervention à distance. Dans ce cas :
 - Les équipements sont reliés à ce point d'accès par un réseau d'administration mis en œuvre soit via un réseau dédié physiquement distinct du reste du SI, soit via une DMZ ou tout autre mécanisme permettant une isolation logique entre les flux d'administration et le reste du SI. Cette isolation logique se fera de préférence au moyen d'un VPN.
 - Le point d'accès distant doit être protégé contre les attaques logiques en provenance des réseaux et son contournement en vue d'accéder au réseau du SI ne doit pas être possible dans la pratique.
 - Le point d'accès doit faire l'objet d'audits de sécurité renouvelés destinés à vérifier sa mise en œuvre et sa résistance aux tentatives d'intrusion dans le SI.
 - Les échanges entre la plateforme d'intervention et le point d'accès distant au SI doivent être 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 responsable du SI de décider, sur recommandation du fournisseur / du prestataire, 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) ;
 - un dispositif de filtrage doit autoriser uniquement les flux nécessaires à l'intervention à distance. Ce dispositif peut être à base de filtrage d'adresse IP ou de liste blanche de certificat par exemple.
- Chaque équipement objet d'une télésurveillance ou d'une télémaintenance doit disposer d'un compte réservé à cette fin et dont les paramètres d'identification et d'authentification sont différents de ceux de tout autre équipement. Tous les comptes existant par défaut doivent être supprimés ou désactivés, ou leurs paramètres d'identification et d'authentification modifiés.
- En cas d'absence prolongée de trafic dans une session, des mécanismes de surveillance doivent clore automatiquement toute session d'échange établie (en direct ou de part et d'autre du point d'accès) entre la plateforme et un équipement objet de l'intervention. Le délai de déconnexion automatique, à convenir en fonction des caractéristiques de l'intervention à distance, doit être aussi court que possible. Si le responsable du SI en a la capacité technique, ces mécanismes sont à mettre en œuvre au niveau du SI. Dans le cas contraire, leur mise en œuvre peut être déléguée par contrat au fournisseur / prestataire qui les met en œuvre à partir de ses équipements utilisés pour les interventions à distance.

- Idéalement, le responsable du SI doit disposer d'un espace de stockage dans lequel les traces des accès et des opérations effectuées à distance sont centralisées et conservées sous son contrôle, en vue d'être exploitées en cas de litige ou d'incident.
- Dans le cas où une centralisation des traces n'est pas possible, le stockage des traces peut s'effectuer sur l'équipement objet de l'intervention y compris dans l'espace de l'outillage mis en œuvre.

ARTICLE 3. MODALITES PRATIQUES DE MISE EN ŒUVRE

Les modalités pratiques doivent être portées à la connaissance des personnes concernées. Elles précisent la prestation en termes de :

- Objectifs et périmètre ;
- Obligations réciproques du fournisseur et du responsable du SI ;
- Moyens mis en œuvre ;
- Procédures ;
- Règles de sécurité.

À ce titre, les dispositions organisationnelles de sécurité suivantes doivent être prises en compte :

- Dans le cas où le responsable du SI ne pourrait pas fournir une liste actualisée et le numéro de téléphone des personnes pouvant solliciter une intervention à distance, des moyens d'authentification des personnes pouvant solliciter une intervention à distance doivent être définis entre le responsable du SI et le fournisseur / le prestataire (ex : n° de contrat associé à un mot de passe).
- La liste actualisée et le numéro de téléphone des personnes pouvant solliciter une intervention à distance doit être communiquée au fournisseur / au prestataire pour permettre à son personnel ou à son sous-traitant de vérifier la validité des demandes d'intervention.
- Les interventions de télésurveillance et de télémaintenance doivent être planifiées. Le filtrage de l'accès distant aux équipements concernés ne doit autoriser l'accès que dans les périodes convenues avec les bénéficiaires de ces interventions. Une procédure d'exception peut être prévue pour autoriser temporairement l'accès en dehors de ces plages, afin de répondre à des besoins d'intervention en urgence.
- Avant d'accorder l'accès, le bénéficiaire d'une intervention de télémaintenance doit s'assurer des dispositions prises sur la sécurité des données et des traitements à définir au préalable par voie contractuelle. À titre d'exemple : sauvegarde préalable à toute intervention, arrêt de la production, isolement de l'équipement, possibilité de retour arrière en cas d'échec de l'intervention, possibilité de contrôler les opérations effectuées etc.
- Toute intervention de télémaintenance doit faire l'objet d'un rapport transmis à son bénéficiaire par le fournisseur / le prestataire, dans les meilleurs délais. La forme du rapport respecte les dispositions du contrat ou, à défaut, est à déterminer lors de la signature du contrat entre l'Etablissement et le fournisseur / le prestataire (document, message électronique de synthèse...). Le mode de transmission du rapport respecte les dispositions du contrat ou, à défaut, est également à déterminer lors de la signature du contrat (envoi par messagerie électronique, mise à disposition sur l'espace client du site du fournisseur...).
- Les interventions de téléassistance s'effectuent sous le contrôle de leur bénéficiaire. Il appartient à chaque bénéficiaire :
 - d'autoriser explicitement la prise de main ou le suivi à distance de son poste de travail (affichage d'une demande d'action d'autorisation sur le poste par exemple) ;

- d'exiger, s'il le souhaite, de moduler l'accès aux données.
- d'être présent et de suivre les actions distantes sur son poste de travail pendant toute la durée de l'intervention.
- Tout bénéficiaire doit avoir la possibilité technique d'interrompre à tout moment la téléassistance en cours et doit avoir été formé sur la mise en œuvre de cette fonctionnalité.

5. Suivi des versions

Version	Date	Nature des modifications
V1	20/12/2022	Création
V2	27/04/2023	Révision par la cellule juridique achats territoriale

6. Circuit de validation

Rédaction	Validation	Approbation
Nom(s) ALANIC Christine Fonction(s) RSSI Date 27/04/2023 Signature	Nom(s) Fonction(s) Date Signature	Mme NAEL Directrice des Projets, de la Qualité et de la Gestion des risques Date Signature

7. Signature fournisseur