



**CHARTRE D'USAGE  
POUR LES  
PRESTATAIRES EXTÉRIEURS ET FOURNISSEURS  
ACCÉDANT AU  
SYSTÈME D'INFORMATION DES ÉTABLISSEMENTS  
DU GROUPE HOSPITALIER DE TERRITOIRE  
LÉMAN MONT-BLANC**

Page Blanche

## CYCLE DE VIE DU DOCUMENT

Charte d'Usage pour les Prestataires Accédant au Système d'Information d'un établissement.		
<b>Référence :</b>		<b>Nombres de pages :</b> 47
Date d'application : 13/11/2020		<b>Classement :</b> Services Qualité : GED établissements
<b>Rédacteur :</b> Jean-Marc EMERAS, RSSI.		<b>Valideur (s) :</b> L. DI TOMMASO : RSSI (Centre Hospitalier Alpes Léman) F. GUILLOT : RSSI (Hôpitaux du Pays du Mont-Blanc) Q. MILANO : RSSI (Établissement Public de Santé Mentale) C. SANCHEZ : RSI (Hôpital Dufresne Sommelier et Hôpital Local de Reignier)
<b>Destinataires pour application :</b> Voir liste de diffusion		<b>Destinataires pour information :</b> Direction
<b>N° Version :</b>	<b>Date :</b>	<b>Nature des modifications :</b>
V1	Janvier 2017	JME - Création
V1.1	Décembre 2017	JME – Référence RGPD + diverses corrections suite aux questions posées par Pierre CARLIER.
V1.2	Août 2018	JME – Relecture avant validation. Divers corrections et ajouts.
V1.3	Août 2019	JME – Formalisation pour le Groupe Hospitalier de Territoire
V1.4	Janvier 2020	JME – fusion avec le document : “Prérequis ENVIRONNEMENT et SECURITE du Système d'Information”.
V 1.5	Janvier 2020	LDT, CSA, FGU, JME – Relecture-Adaptation par RSSI Groupe Hospitalier de Territoire
V2	Octobre 2020	JME – Intégration Analyse de risques et Analyse d'impact sur les données personnelles. Intégration mises à jour de sécurité et délai suite à une annonce de vulnérabilité
V2.1	Juin 2024	LPL – Suppression des annexes et ajout d'un cadre de signature pour les prestataires
V2.2	Septembre 2024	LPL – Suppression du lien avec la charte administrateur/Charte d'usage du système d'information (P.26)

Page Blanche

## LISTE DE DIFFUSION DU DOCUMENT

Destinataires	Date
Directions des Achats GHT et établissements du GHT.	13/11/2020
Directions des Services Économiques du GHT.	13/11/2020
Départements Bio médicaux des établissements du GHT.	13/11/2020
Départements Logistiques des établissements du GHT.	13/11/2020
Départements des Services Techniques des établissements du GHT.	13/11/2020
Services Informatiques des établissements du GHT.	13/11/2020
Tous les partenaires des établissements	13/11/2020
Tous les titulaires de marchés en cours au sein des établissements du GHT	13/11/2020

Page Blanche

## TABLE DES MATIERES

<b>CYCLE DE VIE DU DOCUMENT</b>	<b>3</b>
<b>LISTE DE DIFFUSION DU DOCUMENT</b>	<b>5</b>
<b>TABLE DES MATIERES</b>	<b>7</b>
<b>SIGNATURES</b>	<b>8</b>
<b>1. OBJET</b>	<b>24</b>
<b>2. OBJECTIFS</b>	<b>24</b>
<b>3. CADRE REGLEMENTAIRE – DOCUMENTS DE REFERENCE.</b>	<b>25</b>
3.1. Loi Informatique et Libertés.	25
3.2. Guide d'hygiène informatique.	25
3.3. ANSSI : Recommandations relatives à l'administration sécurisée des systèmes d'information.	26
3.4. ANSSI : Prestataires d'administration et de maintenance sécurisée. Référentiel d'exigences.	26
3.5. Guide ASIP-Santé "Règles pour les interventions à distance sur les systèmes d'information de santé".	26
3.6. Respect du règlement intérieur.	26
3.7. Hygiène et sécurité.	26
3.8. Règlement Général sur la Protection des Données (R.G.P.D.).	27
<b>4. DISPOSITIONS ADMINISTRATIVES GENERALES.</b>	<b>27</b>
<b>5. REGLES REGISSANT LES INTERVENTIONS.</b>	<b>28</b>
5.1. Contraintes de fonctionnement et de continuité de service.	28
<b>6. CONTRAINTES DE CONFIDENTIALITE.</b>	<b>29</b>
6.1. Pendant l'intervention.	29
6.2. Informations et documentations.	31
6.3. En cours de contrat.	31
6.4. Fin de contrat.	31
6.5. Confidentialité.	32
<b>7. ACCES PHYSIQUE SUR SITE.</b>	<b>32</b>
7.1. Accès aux locaux.	33
7.2. Respect des consignes de sécurité	33
<b>8. CONTRAINTES DE SECURITE.</b>	<b>33</b>
<b>9. ACCES DISTANT AU SYSTEME D'INFORMATION.</b>	<b>34</b>
<b>10. SECURITE DU SYSTEME D'INFORMATION</b>	<b>34</b>
10.1. Contrôle d'accès aux locaux.	35
10.2. Réseau	35
10.2.1. Le LAN	35
10.2.2. Le WAN	35
10.3. Authentification.	36
10.4. Sauvegardes.	37
10.5. Disponibilité des informations – PRI/PCI	37
10.5.1. PCI	37
10.5.2. PRI	37
10.6. Installation des matériels.	38
10.7. Antivirus	38
10.8. Cohérence des informations	38
10.9. Mises à jour	39
10.9.1. Systèmes d'exploitation	39
10.9.1. Prestations incluant un ou plusieurs sites Internet.	39
10.9.2. Autres logiciels	39
<b>11. DECRET DE CONFIDENTIALITE. COMPTES UTILISATEURS.</b>	<b>39</b>
<b>12. TELEMAINTENANCE</b>	<b>40</b>
<b>13. GESTION DES CHANGEMENTS / MISE EN PRODUCTION</b>	<b>40</b>
13.1. Gestion des changements	40
13.2. Mise à jour des applications	41
<b>14. ANNUAIRE</b>	<b>41</b>
<b>15. ENVIRONNEMENT TECHNIQUE.</b>	<b>41</b>
<b>16. LES SYSTEMES D'EXPLOITATION.</b>	<b>42</b>
<b>17. SYSTEMES D'IMPRESSION.</b>	<b>42</b>
<b>18. AUDIT DE SECURITE</b>	<b>43</b>
<b>19. DISPOSITIONS PARTICULIERES POUR LA SECURITE DU SYSTEME D'INFORMATION.</b>	<b>43</b>
<b>20. DISPOSITIONS PARTICULIERES CONCERNANT UN PRESTATAIRE FOURNISSANT UN SERVICE EXTERNALISE.</b>	<b>43</b>
<b>21. ENGAGEMENT DE RESPONSABILITE DU PRESTATAIRE</b>	<b>46</b>

## **SIGNATURES**

Les sept établissements du Groupe Hospitalier de Territoire Léman Mont-Blanc listés dans les pages ci-après, représentés par leurs directeurs et directrices respectifs acceptent les termes et décisions tels que rédigés dans le document “GHTLMB - Charte Prestataires V2.docx” :

Les décisions décrites dans ce document s’appliquent dans chaque établissement à la date de signature de son représentant.



Page Blanche

## CENTRE HOSPITALIER ALPES LEMAN

558, route de Findrol  
B.P. 20500  
74130 CONTAMINES-SUR-ARVE



Contamines-sur Arve, le :

13/11/2020

Didier RENAUT  
Directeur



Renaut

Page Blanche

## **HOPITAUX DU LEMAN**

3, Avenue de la Dame  
C.S 20 526  
74203 Cedex THONON-LES-BAINS



Thonon-les-Bains, le : 16/10/2020

Éric DJAMAKORZIAN  
Directeur

Page Blanche

## **HOPITAUX DU PAYS DU MONT-BLANC**

380, rue de l'Hôpital  
74700 Sallanches



**HOPITAUX**  
**DU PAYS DU**  
**MONT BLANC**

Sallanches, le : 09/10/2020

Jean-Rémi RICHARD  
Directeur

Page Blanche

## **ÉTABLISSEMENT PUBLIC DE SANTE MENTALE**

530, rue de la Patience  
CS 20149  
74805 LA ROCHE SUR FORON



**Etablissement Public  
de Santé Mentale 74**

La Roche-sur-Foron, le : 30/10/2020

Florence QUIVIGER  
Directrice.

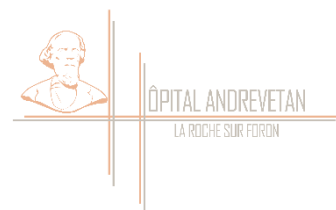




Page Blanche

## **HOPITAL ANDREVETAN**

459, rue de la patience  
74805 LA ROCHE sur FORON



La Roche-sur-Foron, le : 24/09/2020 .

Nathalie POLLEZ  
Directrice

Page Blanche

## HOPITAL LOCAL DE REIGNIER

411, Grande Rue  
74930 REIGNIER



Reignier le : 16/11/2020

Emilie NOEL  
Directrice par intérim.



Page Blanche

## **HOPITAL DUFRESNE SOMMELIER**

498 Route DUFRESNE-  
SOMMEILLER  
74250 LA TOUR



La Tour, le : 13/11/2020

Didier RENAUT  
Directeur.



Renaut

Page Blanche

## 1. Objet

Ce document est la charte d'usage du système d'information (SI) pour les fournisseurs et les prestataires extérieurs appelés à intervenir sur tout ou partie de celui-ci dans l'un ou plusieurs des établissements du Groupe Hospitalier de Territoire Léman Mont-Blanc.

Le présent document constitue une annexe aux marchés et autres commandes publiés ou établis par les établissements du Groupe Hospitalier de Territoire Léman Mont-Blanc (ci-après désigné GHT) comme annexe au Cahier des Clauses Techniques Particulières (CCTP). Il contient la description des règles, des droits, des devoirs et des contraintes informatiques à respecter par les fournisseurs dans le cadre des achats passés par le GHT ou l'un des établissements de ce groupement. Ce document constitue une des pièces du marché. Le simple fait de répondre à la consultation implique l'acceptation, sans restriction, de toutes les clauses prévues dans ce document dans le cadre de la procédure. L'acceptation par un fournisseur d'une commande, résultant d'une consultation quel qu'en soit le type, vaut acceptation des chartes publiées par les établissements du GHT.

Les candidats doivent signaler par écrit, au maître d'ouvrage, toute erreur, omission, imprécision ou contradiction décelée dans ou entre les documents du présent marché. Dans le cas contraire, ce document est considéré comme accepté dans son intégralité.

En cas de litige lié à une différence d'interprétation, c'est l'interprétation de l'établissement acheteur fera foi.

Cette Charte est dite "Charte Prestataires et Fournisseurs" (CPF) dans le corpus documentaire de la sécurité du GHT.

Les clauses d'un CCTP sont réputées confidentielles. À ce titre, elles ne peuvent pas être diffusées à des tiers sous quelque forme que ce soit sans l'accord du maître d'ouvrage.

## 2. Objectifs

Cette charte a pour objet de présenter les règles, droits et devoirs qui sont plus particulièrement spécifiques aux fournisseurs appelés à interagir ou intervenir dans le cadre des réponses au appel d'offres puis de leur mission sur l'un des SI du GHT, ainsi que les contraintes de fonctionnement en place dans les SI des établissements. Ces règles visent à assurer la sécurité et la performance du SI de l'établissement durant leurs interventions que celles-ci se fassent sur site ou à distance. Elles découlent de la Politique Générale de Sécurité du Système d'information (PGSSI) et de la Politique de Sécurité des Systèmes d'Information (PSSI) du GHT.



Le prestataire retenu pour exécuter la mission prévue par la commande, s'engage au strict respect des chartes du GHT et à leurs éventuelles modifications à venir, et aucun ne pourra prétendre les ignorer.

Cette charte s'applique également à tous fournisseurs d'autres équipements qu'ils soient de type biomédicaux, téléphoniques, techniques, logistiques ou autres, dès lors que leurs fournitures disposent de matériels informatiques ou numériques, que ces équipements soient connectés ou pas sur le réseau de l'établissement.

Pour les prestataires déjà engagés avec l'établissement à la parution de ces documents, une version électronique leur a été envoyée afin qu'ils en disposent. La continuation de leurs prestations vaut acceptation de ces chartes.

Au cas improbable où, et seulement dans le cas où aucune solution alternative n'est possible, une clause de cette charte rendrait impossible l'exécution de la mission du fournisseur, une levée de l'exigence incriminée sera étudiée. La levée finale de cette clause ne pourra être faite qu'après accord du RSSI et du DSI et que mention en soit faite dans la mise au point du marché ou de l'achat.

Les règles correspondent aux conditions requises pour que les risques sur la sécurité des informations traitées et sur le fonctionnement du SI restent acceptables lorsque le responsable de ce SI confie des interventions sur site, en télémaintenance, en télésurveillance ou téléassistance à un prestataire.

### **3. Cadre réglementaire – Documents de référence.**

D'une manière générale, il est imposé à tous les prestataires de l'établissement de se conformer aux textes de loi en vigueur. Plus particulièrement :

#### **3.1.Loi Informatique et Libertés.**

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de "loi informatique et libertés" (et ses évolutions) est applicable dès lors qu'il existe un traitement, automatisé ou manuel, contenant des informations relatives à des personnes physiques.

Elle est complétée depuis le 25 mai 2018 par le règlement général sur la protection des données (voir infra).

Ces documents définissent les principes à respecter lors de la collecte, du traitement et de la conservation de ces données et garantissent un certain nombre de droits pour les personnes.

#### **3.2.Guide d'hygiène informatique.**

Ce guide publié par l'ANSI établit les règles de sécurité minimales pour les systèmes d'informations, notamment des entités dépendantes de l'État comme le sont les établissements de santé publics.

### **3.3.ANSSI : Recommandations relatives à l'administration sécurisée des systèmes d'information.**

Ce document publié par l'ANSSI définit les recommandations de l'ANSSI pour les interventions des administrateurs sur les systèmes d'information.

### **3.4.ANSSI : Prestataires d'administration et de maintenance sécurisée. Référentiel d'exigences.**

Ce document permet non seulement aux prestataires de préparer une qualification auprès de cette agence, mais il est également un recueil des bonnes pratiques pour l'administration et la maintenance des SI.

### **3.5.Guide ASIP-Santé "Règles pour les interventions à distance sur les systèmes d'information de santé".**

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.

### **3.6.Respect du règlement intérieur.**

L'ensemble des personnes mandatées par le titulaire est tenu de respecter les règlements intérieurs et les consignes de sécurité générales propres aux différents bâtiments et locaux dans (et éventuellement sur) lesquels il sera appelé à intervenir. En tant qu'annexe du règlement intérieur de l'établissement, l'obligation de respect de la CUSI s'ensuit.

### **3.7.Hygiène et sécurité.**

Le titulaire doit se conformer à l'ensemble des dispositions prévues par le Code du Travail (décret 92-158 du 20-02-92) et par la réglementation en vigueur à la date d'exécution des travaux, l'application desdites dispositions relevant de sa responsabilité.

### **3.8.Règlement Général sur la Protection des Données (R.G.P.D.).**

Les établissements imposent à tous les répondants de fournir en complément de leur dossier un engagement de conformité au règlement général à la protection des données (R.G.P.D.). Des éléments de preuve pourront être fournis avec le dossier de candidature. Il en est de même pour leurs éventuels sous-traitants tout au long du marché.

La société qui se verra attribuer le marché devra impérativement fournir les preuves que les établissements en l'utilisant resteront conformes au RGPD au risque de voir le marché annulé. Ainsi elle fournira :

- La liste de l'ensemble des données personnelles collectées par son application,
- La preuve de licéité du traitement (cas des applications hébergées).
- La preuve de la prise en compte de la sécurité à toutes les étapes du développement.
- La preuve que son outil ne collecte que les données nécessaires au service qu'il assure.
- Que toutes les données sont gérées via un contrôle d'accès et qu'il est possible d'affiner ce contrôle par une gestion de droits (de préférence par profils).
- Que l'historique des données est gérable et que l'établissement pourra définir sa limite de conservation de ces données au besoin de son activité.
- Que l'ensemble des actions est non seulement tracé, mais également facilement auditable à l'aide soit d'un outil spécifique fourni par le titulaire du marché soit d'un outil standard.
- Le cas échéant, l'ensemble de ses sous-traitants pouvant accéder aux données.
- L'usage des données sera limité au traitement pour lequel l'application a été retenue. Tout autre traitement devra avoir reçu l'autorisation écrite de l'établissement contresigné par le DPO.

Si le fournisseur, lors de ses prestations, devient sous-traitant du responsable de traitement au sens du R.G.P.D. ou utilise un nouveau sous-traitant durant le temps du marché, il devra également prouver sa conformité avec cette réglementation.

## **4. Dispositions administratives générales.**

Le titulaire sera responsable du bon fonctionnement de la solution fournie avec une garantie de résultat. Tous les travaux seront effectués dans les règles de l'art, conformément soit aux normes existantes soit aux coutumes et bonnes pratiques de la profession.

Pour l'ensemble du projet, la solution proposée intègre de manière forfaitaire toutes les fournitures et prestations nécessaires à la réalisation complète du projet.

Aucune substitution des services attendus, ni modification des dispositions ne seront tolérées, sauf exception et après autorisation du maître d'ouvrage confirmée par écrit comme prévu au paragraphe "Objectifs".

Le titulaire exécutera sans exception ni réserve, tous les compléments qui sont indispensables pour l'achèvement complet des prestations prévues au titre du marché. Comme déjà précisé, en cas de litige lié à une différence d'interprétation de ce document durant la réalisation des travaux, l'interprétation du maître d'ouvrage fera foi.

Toute prestation présentant des insuffisances vis-à-vis de ce document sera refusée et toutes les conséquences de ce refus (désinstallation, enlèvement, retards, etc. ...) seront à la charge du titulaire.

Le titulaire s'assurera que par ses interventions, il ne dégrade aucune liaison, connexion, équipement ou dispositif en place sur le(s) site(s) au moment de ses interventions. Il s'assurera également que par ces dites interventions, il n'altère pas les qualités intrinsèques des systèmes d'information des établissements dans leur définition la plus large.

Aucun déchet, emballage ou fourniture inutilisée ne seront laissées sur place.

Les éventuels travaux de remise en état des lieux au sens le plus large (immobiliers, mobiliers, numériques...) seront systématiquement à la charge du titulaire.

Toute offre non conforme pourra être écartée.

Toutes les prestations réalisées le sont, soit à partir de la zone de l'Union Européenne, soit en respectant les règles définies par le R.G.P.D. et la C.N.I.L., pour les prestations hors zone de l'Union Européenne.

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 de l'établissement par message électronique aux services économiques, informatiques et maître d'œuvre.

Le fournisseur informe, dès la signature du contrat, l'établissement 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 son sous-traitant, sous son entière responsabilité.

De plus, en cas d'arrêt des activités de la société sans repreneur, le fournisseur s'engage à donner l'ensemble des sources de ses programmes et les documentations techniques et utilisateurs associées aux établissements du GHT utilisant ses produits.

## **5. Règles régissant les interventions.**

### **5.1. Contraintes de fonctionnement et de continuité de service.**

De par leur activité particulière et la permanence de l'accueil des patients, le système d'information des hôpitaux doit être arrêté au minimum et en tout cas pendant les heures où le besoin est le plus faible.

Les candidats et prestataires retenus décriront l'organisation proposée lors de chaque mise en production, pour atteindre cet objectif : enchaînement des étapes de déploiement (sous forme d'un diagramme de Gant et de préférence au format Microsoft Office Project), organisation et dimensionnement des équipes, rôles et charges de l'équipe du maître d'ouvrage. Cette organisation prévisionnelle sera finalisée après une étude détaillée pendant la période de préparation. Un planning et une méthodologie de transfert des installations devront être proposés par le prestataire.

Pour les interruptions de service planifiées, les horaires considérés comme ceux où le besoin des systèmes d'information est le plus faible, sont entre 2H00 et 6H00 du matin. Sous certaines conditions incontournables, les systèmes d'information peuvent être arrêté plus longtemps,

mais dans tous les cas, dans les horaires les moins contraignants pour les professionnels de santé utilisateurs et les plus sécurisants pour les patients.

Les coupures éventuelles seront programmées au plus tôt et au moins 5 jours ouvrés à l'avance.

Pour ces interventions nocturnes, les établissements définissent comme horaires de nuit, la plage comprise entre 22H00 le soir et 7H00 du matin. Il peut aussi être envisagé des coupures les week-end et jours fériés. Dans ce cas, seules les fêtes légales françaises sont prises en compte. Les candidats préciseront s'ils souhaitent surfacturer ces périodes.

Toute intervention se fera conformément à une demande précise décrite soit dans une commande, soit dans un cahier des charges, soit dans un appel au support du prestataire.

Toutes les prestations seront réalisées avec loyauté, discrétion, impartialité et dans les conditions de confidentialité décrites ci-après.

En aucun cas un personnel du prestataire ne pourra faire une opération sur un élément du SI de l'établissement sans que le service informatique de celui-ci n'en connaisse l'identité de l'intervenant, les dates et heures, les motifs, les risques et les procédures à mettre en œuvre pendant et après l'intervention, et que l'ensemble de ces éléments n'aient été validés.

Le fournisseur doit mettre en œuvre les outils nécessaires à la traçabilité des actions de ses intervenants afin d'être, à tout moment, en mesure de déterminer l'identité précise du personnel ayant effectué les opérations sur le SI de l'établissement.

## **6. Contraintes de confidentialité.**

Les données présentes dans les bases des établissements concernent la santé des patients et sont protégées pour la plupart par le secret médical. Il est signifié aux candidats des appels d'offres que tous leurs personnels qui pourront à un moment donné travailler dans l'établissement, ou sur des équipements assurant la circulation ou le stockage de données via une connexion distante, sont tenus au secret professionnel et qu'ils devront respecter la confidentialité de ces informations. Leur responsabilité sera engagée en cas de manquement.

Le titulaire s'engage à observer une stricte confidentialité concernant tout document et toute information en provenance des sites sur lesquels il sera conduit à intervenir. Notamment, ses intervenants ne devront en aucun cas sortir de l'établissement sur quelque support que ce soit partie ou totalité des informations pouvant avoir été accessible durant leur activité, sauf autorisation écrite formelle de l'établissement. Les clauses du présent CCTP sont réputées confidentielles. A ce titre, elles ne peuvent pas être diffusées à des tiers sous quelque forme que ce soit sans l'accord du maître d'ouvrage.

Toute réponse à un appel d'offre touchant de près ou de loin le système d'information implique, en outre, l'acceptation et le respect de la politique de sécurité et de la charte informatique des établissements.

### **6.1. Pendant l'intervention.**

Le fournisseur s'engage formellement à :

- Ne dégrader aucune liaison, connexion, matériel, logiciel ou dispositif en place sur site au moment de ses interventions. Il devra en particulier mettre en œuvre les moyens et procédures conformes aux règles de l'art pour éviter les incidents.
- Ne pas altérer les qualités intrinsèques des autres ouvrages (degré coupe-feu, isolement acoustique, résistance mécanique, etc...) et équipements. En cas de dégradation, ces ouvrages devront être reconstitués. La réception de ces travaux sera faite par les services compétents de l'établissement.
- Programmer les coupures éventuelles au plus tôt et au moins 5 jours ouvrés à l'avance. N'effectuer aucune coupure sans l'accord du DSI ou du technicien en charge de son intervention.
- Sauf exception validée par le DSI, ne pas travailler sur les systèmes en production sans phase de validation des modifications sur un environnement de test adapté. Ne pas effectuer de mise en production sans l'accord du DSI ou du chef de projet.
- Ne pas tenter par quelque moyen que ce soit de contourner ou arrêter un système de sécurité en place.
- Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat.
- Tous les travaux seront exécutés selon les règles de l'art, conformément aux normes et décrets en vigueur portant sur les installations décrites ci-après.
- Il est entendu que le titulaire se sera rendu compte de l'ampleur des opérations et des contraintes à effectuer, de leur importance, de leur nature et qu'il aura suppléé, par ses connaissances professionnelles, aux détails qui pourraient être omis sur les descriptifs et additifs éventuels du document de consultation.
- Fournir tous les équipements avec la dernière version logicielle validée par le constructeur notamment du point de vue des correctifs de sécurité.
- Disposer des qualifications officielles, agréments et certifications nécessaires à l'exécution des opérations qu'il s'engage à exécuter. Que son personnel soit dument qualifié, formé et habilité selon les exigences propres à chaque spécialité nécessaire à l'exécution de l'ouvrage.
- Veiller à l'application stricte des dispositions d'hygiène et de sécurité, et exercer une surveillance continue sur le chantier à l'effet d'éviter tout accident aux personnels travaillant sur ledit chantier, à quelques corps d'état qu'ils soient rattachés, aux personnes employées à un titre quelconque sur le chantier, ainsi qu'à celles qui sont étrangères à celui-ci, et notamment les occupants normaux des locaux et des espaces publics sur lesquels se déroule le chantier.
- Prendre la responsabilité de tous les accidents ou dommages causés à toute personne en général, résultant soit d'une faute dans l'exécution de ses travaux, soit du fait de ses employés
- Garantir le maître d'ouvrage contre tout recours qui peut être exercé contre lui, du fait de l'inobservation par le fournisseur ou un membre de son personnel de l'une quelconque de ses obligations.
- 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 maître du fichier est nécessaire.
- Ne recourir qu'aux méthodes outils et techniques présentées en phase projet, validées par l'établissement.
- De signaler formellement au DSI et au RSSI tout contenu manifestement illicite qu'il peut découvrir dans le cadre de sa prestation



## **6.2. Informations et documentations.**

Le fournisseur s'engage formellement à :

- Fournir un dossier technique d'exécution.
- Ne prendre aucune copie des données, 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 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 de sécurité, notamment matérielle, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat.
- Apporter toutes les réponses aux questions que peuvent se poser les établissements dans leur analyse de risques (AR) liée à l'implantation du nouveau service ainsi que pour l'analyse d'impact sur la protection des données personnelles (AIPD).

## **6.3. En cours de contrat.**

Le prestataire s'engage à :

- Signaler les vulnérabilités des éléments composant sa fourniture dont il a connaissance.
- Lutter contre la propagation de codes malveillants ou d'incidents de sécurité à partir de sa plateforme.
- Restreindre l'accès au SI de l'établissement aux seuls intervenants déclarés.
- Ne répondre qu'aux demandes des personnes autorisées par l'établissement à le solliciter. Ces personnes seront listées en début de contrat.
- De ne pas accéder au SI de l'établissement autrement que par les moyens spécifiques mis en place en début de contrat.

## **6.4. Fin de contrat.**

Le fournisseur s'engage à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations de l'établissement dont il pourrait avoir une copie sur un quelconque support.

Dans le cas de la reprise de matériel, il s'engage à détruire ces matériels selon les règles de l'art et les conseils de l'ASIP santé publiés dans le "Guide pratique spécifique à la destruction de données lors du transfert de matériels informatiques des Systèmes d'Information de Santé".

À la fin du contrat, le fournisseur donnera un rapport d'intervention précisant l'ensemble des opérations menées.

## **6.5. Confidentialité.**

Les données présentes dans les bases des établissements concernent pour la plupart la santé des patients et sont en conséquence protégées par le secret médical. Il est signifié aux candidats des appels d'offres que tous leurs personnels qui pourront à un moment donné travailler dans l'établissement, ou sur des équipements assurant la circulation ou le stockage de données via une connexion distante, sont tenus au respect de la confidentialité de ces informations. Leur responsabilité d'employeur sera engagée en cas de manquement.

Le fournisseur et les membres de son personnel sont donc tenus au secret professionnel et au secret médical. Ils s'engagent en particulier à n'utiliser les documents et informations fournis par les établissements du GHT que dans le cadre des prestations pour lesquelles ils ont été mis à disposition. Ils s'engagent à observer une stricte confidentialité concernant tout document et toute information en provenance des sites sur lesquels il sera conduit à intervenir. Le fournisseur est responsable de l'usage des informations auxquelles son personnel peut avoir accès. Il est encouragé à ce que chaque intervenant (sur site ou à distance) signe un engagement individuel de confidentialité annexé à son contrat de travail. Il est souhaitable que cet engagement fasse apparaître la notion de confidentialité des données médicales. Il est particulièrement souligné que cette exigence de confidentialité est sans limite dans le temps et, notamment, ne s'arrête ni à la fin de la prestation liant l'intervenant à l'établissement, ni à la fin du contrat de travail d'un des employés. L'engagement de confidentialité devra faire une mention précise de ce point.

Le fournisseur est responsable vis-à-vis des actions que son personnel peut effectuer. Chaque personne concernée devrait également avoir signé un engagement individuel de limitation de ses actions au seul besoin des interventions.

Le fournisseur s'engage à ne faire des copies de données que si son intervention l'impose et à n'en conserver aucune à la fin de son intervention.

Les intervenants ne devront en aucun cas sortir de l'établissement, sur quelque support que ce soit, partie ou totalité des informations pouvant avoir été accessible durant leur activité, sauf autorisation écrite formelle de l'établissement.

## **7. Accès physique sur site.**

De même que le service informatique fourni les chartes liées au SI, le service sécurité de l'établissement joint à toutes les consultations les règles applicables lors d'interventions dans les locaux.

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.).

Ces 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, du service biomédical, des services techniques ou du service sécurité.



- 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.

### **7.1.Accès aux locaux.**

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

### **7.2.Respect des consignes de sécurité**

Le fournisseur s'engage au respect des consignes de sécurité de l'établissement fournis en annexe du CCTP et en particulier, les consignes ci-dessous :

- Au niveau de la sécurité :
  - les zones à risques sont balisées,
  - les outils électriques et/ou tranchants utilisés sont aux normes en vigueur,
  - les sorties de secours ne doivent pas être obstruées.
- Au niveau de l'hygiène :
  - les sanitaires utilisés sont ceux que le maître d'ouvrage met à la disposition du titulaire.
  - le chantier est rangé et nettoyé après chaque journée de travail.
  - Les emballages seront évacués au fur et à mesure de telle sorte à ne pas encombrer les circulations et autres locaux.

## **8. Contraintes de sécurité.**

Les candidats répondants aux appels d'offres s'engagent à tout mettre en œuvre afin de garantir que la continuité des systèmes d'information ne soit pas interrompue suite à l'opération d'un matériel, d'un logiciel ou d'un personnel sous leurs responsabilités ou de leurs fournitures.

D'autre part les candidats s'engagent à se conformer aux plans de prévention et conditions d'accès en vigueur dans chacun des établissements du G.H.T.

Enfin, les candidats présenteront une attestation d'assurance couvrant leur responsabilité en cas d'incident portant préjudice aux établissements ou aux personnes les fréquentant pour quelque raison que ce soit.

## **9. Accès distant au système d'information.**

Le fournisseur doit fournir une liste nominative actualisée des personnes pouvant solliciter une intervention à distance.

Chaque personne devra travailler avec les identifiants qui lui seront fournis. Les identifiants sont personnels. En cas d'incident, le titulaire de l'identifiant de connexion devra assumer la responsabilité des opérations faites avec son compte.

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, autant que faire se peut, les accès physiques et logiques des postes d'intervention aux seules personnes autorisées.

S'il le désire, l'établissement 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. Il assure la traçabilité des opérations faites durant le délai légal imposé pour les données accédées par son intervenant (celles de ses équipements comme celles des établissements), donc le cas échéant, après le départ d'un employé.

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 SI
- 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 SI de l'établissement soient effacées de la plateforme.

Toute intervention de télémaintenance doit faire l'objet d'une communication transmise au service informatique avant chaque connexion et en indiquer la raison.

## **10.Sécurité du système d'information**

Les centres hospitaliers ont mis en place un certains nombres de matériels et procédures pour assurer au maximum la sécurité de leur SI respectif. Les règles qui en découlent s'appliquent à tout nouveau système et à tous les intervenants appelés à travailler sur site ou en télémaintenance sur les systèmes d'information, au sens large, des établissements du G.H.T.

L'évolution de la sécurité suit dans tous les cas, et a minima, les recommandations, instructions, et législation imposées par l'administration centrale. Les attributaires des marchés devront collaborer avec les établissements pour la mise en place des règles qui pourraient s'imposer à leurs fournitures.

## **10.1. Contrôle d'accès aux locaux.**

Les établissements disposent d'un contrôle d'accès pour leurs salles informatiques ainsi que pour les locaux techniques afin d'assurer la sécurité physique de leurs équipements. Seuls les agents habilités des établissements peuvent accéder à ces locaux non accompagnés.

## **10.2. Réseau**

### **10.2.1. Le LAN**

Pour l'ensemble des sites, le protocole déployé est "Ethernet" et le moyen de transport est "TCP/IP".

Les réseaux sont sécurisés par duplication des équipements les plus sensibles et redondance des liens.

Dans chaque établissement, le réseau dispose d'un plan d'adressage privé conforme à la RFC 1918 avec distribution automatique des adresses IP.

L'infrastructure réseau est imposée.

### **10.2.2. Le WAN**

#### **10.2.2.1. Le réseau intersites.**

Les établissements disposent de liens entre leurs différents sites. Ces liens font l'objet de marchés indépendants les uns des autres dans l'attente d'une convergence des SI. Le titulaire devra travailler en collaboration avec les sociétés qui se sont vues attribuer ces marchés en cas d'actions touchant à la configuration de ces liens.

#### **10.2.2.2. Les liens Internet.**

Les établissements disposent d'un accès sécurisé vers Internet. Cet accès est en règle générale fait par l'intermédiaire d'un système de firewall qui est centralisé sur le site principal. Là encore, les marchés en cours sont différents et les solutions implantées le sont aussi. Une convergence est planifiée.

### **10.2.2.3. Le réseau d'interconnexion des établissements.**

Une interconnexion entre les réseaux du Centre Hospitalier Alpes Léman, des Hôpitaux du Léman, l'Hôpital Andrevetan, l'Établissement Public de Santé Mentale et des Hôpitaux du Pays du Mont Blanc a été mise en place. Elle est amenée à être étendue vers d'autres établissements dans le cadre du GHT. À ce jour, les plans d'adressage des établissements ont des plages d'adresses qui se chevauchent. Il y a donc des technologies de translation d'adresses (N.A.T.) sur ces liens. Ces liens s'appuient sur les technologies disponibles dans les systèmes de firewall des établissements. Un projet est en cours depuis le 4ème trimestre 2019 pour revoir la segmentation réseau, et en même temps, supprimer ces chevauchements.

### **10.2.2.4. Internet Patients.**

Plusieurs établissements fournissent un accès internet à leurs résidents. Cet accès internet s'appuie sur l'infrastructure des établissements. En conséquence une coupure du réseau non seulement arrête les professionnels, mais également les patients qui ont une connexion internet. Celle-ci étant parfois facturée, ces arrêts doivent être encore plus limités.

## **10.3. Authentification.**

L'accès au réseau dépend d'un identifiant et d'un mot de passe attribué par le service informatique. Les comptes sont personnels. Les droits associés à ces comptes dépendent d'une matrice de droits établie par le groupe dédié à la gestion des droits. Les candidats proposant un service de maintenance (en présentiel ou distant) ne pourront prétendre qu'au droits jugés nécessaire à leur activité. Un compte par intervenant extérieur sera attribué à des fins de traçabilité.

Les établissements du GHT savent qu'il leur faudra faire évoluer leur système d'authentification vers un système à double facteur ce qui devrait se faire par la mise en place d'un badge pour se connecter au réseau. Dès à présent, chaque établissement dispose d'un système de badge avec comme cible que les utilisateurs n'aient qu'un seul badge pour tous les besoins dans l'établissement (contrôle d'accès, pointage, restaurant du personnel,...).

Ces badges ne servent pas actuellement pour l'authentification sur le réseau, mais leur évolution dans ce sens, sur chaque site, se fait de façon concertée afin que les utilisateurs n'aient, à termes, qu'un seul badge quel que soit l'établissement où ils sont appelés à effectuer leur mission.

En conséquence, si la solution proposée comporte une fonctionnalité reposant sur l'utilisation d'un badge personnel, celui-ci devra être compatible avec la technologie de badge cible, MIFARE, et le fournisseur devra se conformer aux règles de paramétrage de la mémoire de ce type de cartes, en cours dans les établissements.

## **10.4. Sauvegardes.**

Les établissements disposent de système de sauvegarde et d'un plan de sauvegarde. La solution qui sera retenue dans le cadre de cet appel d'offre devra s'intégrer dans ces plans de sauvegarde sans imposer l'équipement de nouveaux matériels.

## **10.5. Disponibilité des informations – PRI/PCI**

### **10.5.1. PCI**

De par leur activité spécifique, les centres hospitaliers tendent à mettre à disposition de leur professionnels un SI fonctionnant 24/24H et 7/7J. Pour cela, l'ensemble de leurs projets incluent un plan de continuité d'activité Informatique (PCI) pour le nouveau service. Ce PCI est défini comme une architecture sécurisée permettant d'assurer le service attendu sans interruption. Les PCI de toutes les applications sont mis en cohérence les uns par rapport aux autres pour constituer le PCI de l'établissement assurant ainsi la partie informatique du plan de continuité d'activité global de l'établissement (PCA).

In extenso, la cible est de mettre en place une installation capable de fonctionner 100% du temps malgré les pannes des matériels et les besoins de maintenance ou d'exploitation (mises à jour des différents logiciels, redémarrages des matériels...). Les centres hospitaliers privilégient les configurations permettant un PCI actif/actif, réparti sur leurs deux salles informatiques.

### **10.5.2. PRI**

A ce PCA, les établissements couplent un plan de reprise d'activités (PRA) global. Il en est de même pour le SI qui se double d'un plan de reprise d'activités informatique (PRI), également par application, qu'ils définissent comme un ensemble exhaustif de procédures écrites, contenant les paramètres précis de l'équipement fourni, des données gérées par l'application, des pannes pouvant survenir, des méthodes pour enregistrer les données le temps de l'interruption, la façon de gérer l'incident et de redémarrer dès que les conditions sont revenues. Ces procédures permettent d'assurer la continuité du service lors de tout incident majeur entraînant un arrêt malgré le PCI. Elles décrivent les procédures dégradées, leur mise en œuvre, les opérations à mener et leur la chronologie pour revenir à la situation normale ainsi que les actions à entreprendre suite à la résolution de l'incident.

Chaque procédure est attachée à un type d'incident et comprend :

- Le type d'incident, exemple : perte d'un serveur
- Les conséquences attachées, exemple : des performances dégradées, des utilisateurs sans téléphone, des professionnels n'ayant pas accès aux plan de soins...
- La liste des utilisateurs impactés, exemple : ensemble du service du personnel, M. X, Mme Y, le site S....

- Les actions à entreprendre pour assurer la continuité, exemple : démarrer la procédure dégradée N°...,
- Les actions à entreprendre pour revenir à un fonctionnement normal. Exemple :
  - Appel du support du fournisseur selon procédure N°...
  - Déclenchement de la procédure dégradée N°...
  - Convocation de la cellule de crise.
  - Déclaration du matériel en panne et demande d'intervention ou installation du matériel en spare selon les procédures N°X, Y..., puis demande de renouvellement du matériel de spare selon procédure N°...
  - Redémarrage du nouveau matériel,
  - Vérification du fonctionnement,
  - Réinstallation de la dernière configuration,
  - Remise en fonction du serveur,
  - Reprise ou ressaisie des données modifiées pendant la panne,
  - Passage en environnement normal,
  - Retour du matériel défectueux,

Compléter le PCI et le PRI fait partie des tâches de tout projet SI. Sauf mention contraire, ces prestations sont demandées au fournisseur ou à l'intégrateur de toute nouvelle solution. Cette notion est désormais d'autant plus sensible que le R.G.P.D. demande que les projets soient menés avec une philosophie de Privacy On Design (prise en compte des contraintes de sécurité des données personnelles dès la conception du service).

## **10.6. Installation des matériels.**

Les salles informatiques sont organisées en général à l'aide d'armoires racks au format 19". L'ensemble des matériels qui sont installés dans ces salles, sont donc dans ce format. Ils peuvent-être sur rails coulissants et disposent un minima de double attachement électrique. Il en sera de même pour tous les matériels proposés dans le cadre d'un marché.

## **10.7. Antivirus**

Les centres hospitaliers sont équipés de systèmes d'antivirus. Tout nouveau matériel placé au sein des du G.H.T. devra être compatible avec les systèmes antivirus en place et leurs mises à jour automatiques. Si la fourniture exige des exclusions, la liste de ces exclusions concernées devra lors de la remise du dossier de consultation.

## **10.8. Cohérence des informations**

Les établissements ont mis en place un certain nombre de procédures pour assurer la cohérence des informations saisies.

## **10.9. Mises à jour**

### **10.9.1. Systèmes d'exploitation**

Selon l'instruction 309, tous les systèmes d'exploitation en usage doivent être dans une version maintenue par l'éditeur. Les patches de sécurité fournis par l'éditeur seront déployés au plus vite. L'attention des fournisseurs est attirée sur les patches Tuesday de Microsoft dont les KB de sécurité seront installées dès que la production le permettra et au plus tard dans les 8 jours après la parution.

### **10.9.1. Prestations incluant un ou plusieurs sites Internet.**

Les sites ouverts sur Internet étant particulièrement exposés, les prestataires devront impérativement concevoir ou avoir conçu leurs sites en prévoyant les mises à jour de sécurité de l'ensemble des composants Web de sa prestation. Ces mises à jour devront être installées dès leur disponibilité. La liste complète des composants sera fournie lors de la mise en place afin que le suivi des mises à jour puisse se faire facilement.

### **10.9.2. Autres logiciels**

Les prestataires s'efforceront de maintenir leurs logiciels devant utiliser des produits standards dans la dernière version publiée de ceux-ci, tout particulièrement lors d'évolution consécutives à des mises à jour de sécurité pour des failles 0-DAY.

Lors de découvertes de failles de sécurité, le prestataire devra mettre en œuvre tous les moyens possibles pour réduire au maximum le délai entre l'annonce et le déploiement du correctif. Dès lors que la faille touchera des données personnelles ou de santé, le délai d'installation du correctif devra être réduit à 8 jours maximum.

## **11. Décret de confidentialité. Comptes utilisateurs.**

Comme l'ensemble des hôpitaux, les établissements membre du GHT doivent mettre en place les contraintes découlant du décret de confidentialité et du R.G.P.D. Dans ce sens, ils doivent travailler à la suppression des comptes génériques. Dans le même objectif de réponse, et également pour simplifier les connexions de leurs utilisateurs, notamment mobiles, les établissements évolueront dès que possible vers un système d'authentification forte et unique basé sur un annuaire unique.

Les établissements ont mis en place un contrôle d'accès aux informations numériques basé sur des rôles d'utilisateurs selon les métiers. Cette politique RBAC (Role Based Access Control)/OrBAC (Organisation Based Access Control) détermine les droits d'accès aux



données en fonction des métiers des utilisateurs. Cette politique décide également des droits d'accès des partenaires en fonction de leur fourniture.

## **12. Télémaintenance**

Sur demande des fournisseurs et prestataires, des accès en télémaintenance peuvent être autorisés par les services informatiques des établissements. Ces accès se feront selon les règles en place pour chaque SI. Les prestataires ne pourront prétendre qu'aux accès nécessaires pour la maintenance des équipements fournis. Ces accès seront enregistrés et contrôlés. Les plages horaires d'ouverture et les droits nécessaires seront accordés selon les besoins.

L'accès par d'autres logiciels de prise en main à distance devra être validé par le responsable de la sécurité du SI du GHT ou du correspondant RSSI local et le directeur en charge de l'informatique de chaque établissement.

## **13. Gestion des changements / Mise en production**

### **13.1. Gestion des changements**

Avant toute mise en production, les applications font l'objet d'un certain nombre de contrôles :

- Disponibilité des postes de travail nécessaires
- Validation des tests sur les serveurs de production
- Disponibilité des besoins d'infrastructure, notamment le "capacity management".
- Identification complètes des utilisateurs finaux et impactés.
- Disponibilité des comptes et des droits d'accès.
- Disponibilité par le service informatique des spécificités techniques, du cahier d'exploitation, du PCI et du PRI, des procédures d'appels au support du fournisseur.
- Le niveau de service contractualisé
- L'identification précise des utilisateurs référents
- La validation de la fin de paramétrage de l'application par le chef de projet
- La validation des interfaces.
- La description des actions techniques nécessaires à la mise en production et l'identification des intervenants en ayant la charge.
- La fin des tests de fonctionnement et la levée de toutes les réserves bloquantes pour le démarrage. Notamment des tests de montée en charge.
- La fin des formations des utilisateurs permettant leur maîtrise dans les procédures d'identification dans l'application et un usage journalier de celle-ci.
- Le cas échéant de la séparation des environnements de tests et de production.
- L'identification du responsable de l'accompagnement au changement



L'ensemble de ces contrôles permettant une validation du démarrage en comité de pilotage et d'obtenir l'accord signé de mise en production du Directeur en charge du projet ou du représentant du pouvoir adjudicateur du projet concerné.

### **13.2. Mise à jour des applications**

Le processus de gestion du changement implique fortement les métiers. Les modifications de l'environnement de production font l'objet d'un suivi systématique.

Avant chaque mise à jour, les établissements procèdent à un contrôle des points suivants :

- Identification précise des logiciels mis à jour, des serveurs et des postes de travail concernés ainsi que des correspondants de l'application.
- Les services destinataires de la mise à jour
- L'impact sur l'ensemble du SI.
- L'identification des intervenants
- La procédure de mise à jour et la voie de mise en place (sur site ou par télémaintenance)
- L'existence des prérequis humains, techniques et logiciels.
- La validation de la mise à jour en environnement de test (de la procédure de mise à jour et des fonctionnalités de l'application, nouvelles comme anciennes).
- La détermination des temps d'arrêt.
- Les possibilités de retour arrière.
- La planification.
- Les besoins en formation complémentaire.

L'ensemble de ces points permettant d'obtenir la validation signée du responsable informatique du site.

## **14. Annuaire**

Les établissements ont mis en place un annuaire d'entreprise Microsoft Active Directory et travaillent sur un projet I.A.M. Il est utilisé comme base de comptes utilisateurs pour les domaines Microsoft et pour toutes les applications des SI qui supportent ce service.

## **15. Environnement technique.**

La prise en compte de l'environnement informatique des établissements (logiciel, infrastructure, équipements biomédicaux, GCS laboratoire, sécurité, etc.) dans toute nouvelle mise en place de solution est indispensable. Le travail en collaboration avec les supports logiciels métiers et tous les partenaires des centres hospitaliers peut être nécessaire et imposé dans les phases d'intégration.

Les établissements disposent généralement d'un contrat de support chez leurs éditeurs pour leurs applicatifs métiers et la plupart des logiciels qu'ils utilisent.

## **16. Les systèmes d'exploitation.**

Les systèmes d'exploitation en place sont :

- Windows serveur (2008R2, 2012R2, 2016). Quelques serveurs Windows de versions antérieures sont en cours de migration. L'objectif est de respecter l'instruction 309 au plus vite.
- Linux (Red-Hat, CentOS, etc.)

Parmi ces serveurs, certains sont contrôleurs de domaine Active Directory.

Les établissements membres du GHT imposent aux candidats des solutions parfaitement compatibles avec l'environnement existant et historique installé sur leurs sites.

Pour les établissements ayant un domaine Active Directory Windows, sont exclues les solutions sous Windows Small Business Server.

Conformément à l'instruction 309, les centres hospitaliers imposent, dans le temps, que les solutions fournies ne fonctionnent que sur des systèmes d'exploitation supportés par leurs éditeurs. De par l'obligation légale de cette mesure, les évolutions nécessaires des produits fournis devront être mises à disposition sans surcoût.

Les centres hospitaliers imposent également que leurs systèmes d'exploitation restent à jour des correctifs de sécurité publiés par les éditeurs. Les titulaires des marchés s'engagent à faire évoluer leurs applications afin qu'elles soient opérationnelles avec ses nouveaux correctifs cela dans le cadre de leur contrat de maintenance de base, donc sans surcoût.

## **17. Systèmes d'impression.**

Le Groupe Hospitalier de Territoire dispose d'un marché pour l'ensemble de ses systèmes d'impression. Celui-ci prévoit différents modèles. En conséquence, ceux-ci sont imposés.

Dans les cas très particuliers où, sur l'ensemble des systèmes d'impressions, aucun modèle ne conviendrait, et à défaut d'une solution concurrente techniquement équivalente et permettant le respect du marché des systèmes d'impression, les établissements du GHT accepteraient le modèle imposé par le fournisseur. En contrepartie, celui-ci devra mettre en place un système complet de mise à disposition, de maintenance et de fourniture de consommables. Il devra également prévoir la continuité de service de ce matériel en fonction de sa sensibilité dans le processus de soins.

## **18. Audit de sécurité**

Afin de répondre aux prérequis du programme HOP'EN auquel des établissements du GHT candidatent, tous les établissements font réaliser annuellement un audit de sécurité sur leur infrastructure.

Les répondants aux appels d'offres devront présenter des offres qu'ils garantiront passer ces audits. Dans le cas contraire, le candidat devra, à ses frais, mettre en place l'ensemble des correctifs de sécurité nécessaires au retour au niveau de sécurité existant avant leur installation.

Dans le cas particulier des équipements bio médicaux, dont les mises à jour de sécurité dépendent d'un agrément C.E., ce point sera revu au cas par cas.

## **19. Dispositions particulières pour la sécurité du système d'information.**

L'établissement met à disposition de ses fournisseurs un moyen d'accès distant sécurisé. Si ce point d'accès 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. Ces échanges doivent être protégés de bout en bout par des fonctions de chiffrement et d'authentification mutuelle. Les connexions du télémainteneur sur les équipements contenant des applications ou des informations à caractère personnel doivent se faire uniquement selon les modalités prévues entre lui et l'établissement.

Avant chaque intervention, le télémainteneur doit informer le service informatique (mail ou téléphone) et demander une autorisation d'accès. Il informe l'établissement de chaque opération de maintenance dont il prend l'initiative (natures des opérations, noms des intervenants). En cas de complications, il tient informé la DSI des difficultés et solutions mises en œuvre. En fin d'intervention il fait parvenir un rapport d'activité listant l'ensemble des opérations effectuées.

Le point d'accès distant est protégé contre les attaques logiques en provenance des réseaux et les outils de protection ne doivent pas être contournés.

Tout accès distant est tracé et les enregistrements conservés pour une durée correspondant à la législation.

Chaque équipement objet d'une télésurveillance ou d'une télémaintenance dispose de comptes réservés à cette fin (un par intervenant déclarés) et dont les paramètres d'identification et d'authentification sont différents de ceux de tout autre équipement. Ces identifiants sont confidentiels et ne doivent pas être prêtés à d'autres intervenants de la même société ou de toute autre. Ces identifiants engagent la responsabilité juridique de l'intervenant.

## **20. Dispositions particulières concernant un prestataire fournissant un service externalisé.**

Lorsque l'établissement à recours à une solution hébergée, le fournisseur s'engage sur :

- La performance du service (temps de réponse lié à la capacité réseau et à la bande passante...),

- La disponibilité du service (temps de traitement des pannes correspondant à des niveaux de service...),
- La sécurité du service et des données (intégrité des données dépendant des procédures de sécurité, et de cryptage des données sensibles...). Le fournisseur fournira son plan d'assurance sécurité. Dès lors qu'il s'agira de données médicales, la solution devra être conforme aux exigences concernant l'hébergement des données médicales, de la législation en cours.
- La confidentialité des accès et des données. Les informations saisies dans l'application hébergées mise à disposition par le fournisseur sont couvertes par le secret professionnel et souvent également par le secret médical. L'accès à ces données par le personnel du fournisseur ne pourra se faire que dans le cadre d'une opération d'administration ou d'un support aux utilisateurs. IL est précisé que le paragraphe concernant la confidentialité de ce document s'applique également dans ce cas.
- La traçabilité des accès. Outre la traçabilité qui sera mise en place pour les utilisateurs de l'établissement, le fournisseur devra à tout moment être en capacité d'identifier l'auteur d'une action (personnel d'un des établissements ou membre de son propre personnel) sur une donnée et de prouver cet accès. Dans le cas d'un membre de son personnel, il devra également être capable de prouver que cette action a eu lieu dans le cadre des opérations d'administration normales du service. Cette traçabilité devra être disponible sur la durée légale d'enregistrement, soit, à la parution de cette charte, un an.
- Sauvegarde / restauration. La contractualisation du service déterminera un RTO et un RPO. Le prestataire fournira en conséquence un plan de sauvegarde correspondant et les procédures de tests de restauration et de redémarrage après une panne majeure. Le prestataire s'engagera sur la réalisation de tests à blanc au moins une fois par an. Les établissements pourront exiger être présent le jour de ces tests.

Page Blanche

## 21.Engagement de responsabilité du prestataire

Je soussigné(e) .....,  
responsable en qualité de .....,  
certifie avoir pris connaissance de la Charte Prestataire et m'engage à ce qu'elle soit appliquée  
lors de toute mission ou intervention confiée par un, plusieurs ou tous les établissements  
composant le GHT Léman Mont-Blanc dans le cadre du contrat auquel est joint cette charte.

Au-travers de cette signature, je certifie également avoir le pouvoir d'engager la société que je  
représente.

Fait à .....

Le .....

Cachet du Prestataire et signature du responsable précédé de la mention « Lu et Approuvé »



**Groupe Hospitalier de Territoire**  
**LEMAN - MONT-BLANC**