

ELEMENTS DSI

GENERALITES :

Pour les composantes informatiques de sa proposition, le fournisseur devra se conformer strictement aux attentes spécifiées dans les sous-chapitres suivants. En cas de non-conformité, il devra clairement identifier cette non-conformité et expliciter son choix.

De manière générale, le fournisseur décrira précisément les composants informatiques de sa proposition, ses spécifications, les modes d'installation, de support et d'évolution des versions.

Notamment les différents produits devront répondre aux exigences de sécurité suivantes :

- versions supportées par les éditeurs uniquement et maintient dans le temps de ces versions à jour
- antivirus sur les systèmes d'exploitation
- détail de tous les flux réseau utilisés et durcissement des systèmes par désactivation des services inutiles

1 SERVEURS

Général

- La virtualisation est à privilégier, sauf nécessité technique
- Les machines virtuelles seront hébergées sur les infrastructures du CHU qui utilisent exclusivement l'hyperviseur NUTANIX AHV
- Si l'offre nécessite un serveur physique, le CHU pour des raisons d'homogénéité de son parc fera de préférence l'acquisition sur ses marchés propres
- Si l'offre comprend obligatoirement la fourniture d'un serveur physique, pour pouvoir être hébergé dans le datacenter du CHU, il devra :
 - o être en format rack 19 pouces
 - o posséder des alimentations redondantes
 - o proposer des cartes réseaux redondantes, mode teaming (également supportée par l'OS et l'ensemble de la solution logicielle)
- Le CHU possède ses propres marchés pour les licences Microsoft, elles ne doivent donc pas être fournies dans l'offre
- Les spécifications détaillées des serveurs doivent à minima comprendre :
 - o indications CPU
 - o mémoire RAM
 - o Disques et partitions
 - o performances disques attendues
 - o OS (préciser version française ou anglaise)
- Le CHU supporte et peut installer les OS suivants : Windows 2016, Windows 2019, Redhat 7 et 8, Centos 7 et 8

Les serveurs devront être joints au domaine Active Directory du CHU pour permettre l'authentification nominative des administrateurs. Les serveurs Windows héritent alors de l'antivirus Microsoft et des mises à jour automatiques

2 STOCKAGE NAS

- Pour des besoins de stockage, un partage NAS peut être mis à disposition par le CHU sous réserve de disponibilité
- Ce partage peut être disponible en NFS ou CIFS. Dans ce dernier cas, les droits sont affectés sur la base d'un compte Active Directory.
- Un mode WORM peut permettre l'archivage. Les modalités précises de mise en œuvre seront à valider.

A. BASES DE DONNEES

- Le CHU supporte les bases de données Oracle et Microsoft SQLServer.
- Les versions des moteurs de bases de données devront être officiellement supportées par l'éditeur et évoluer dans le cadre de la maintenance pour le rester.
- Le CHU pourra décider d'héberger les bases sur ces serveurs centraux de base de données pour des raisons de plan de reprise
- Si le candidat propose un autre type de base de données, il devra assurer le support, la sécurité et l'exploitation : évolutions, maintenance, sauvegarde, restauration, surveillance.

B. TELEMAINTENANCE

- Le fournisseur devra utiliser le portail SSL IPDiva mis à disposition par le CHU
- Seulement sur dérogation accordée par le CHU suite à étude technique, une autre solution justifiée pourra être utilisée
- Les comptes utilisateurs sont nominatifs. Il est nécessaire de fournir un numéro de téléphone portable ou à défaut une adresse mail individuelle pour obtenir le code OTP
- Sur exception justifiée, un compte générique et une adresse mail générique peuvent être utilisés (uniquement pour des plateformes de support)
- Les sessions de télémaintenance sont enregistrées

C. RESEAU

- Le réseau filaire 100/1000 Mb/s
- Réseau WIFI :
 - o Couverture des zones de circulation
 - o Privilégier bande des 5Ghz
- Sécurisation 802.11x
 - o Sur la base d'un compte utilisateur AD
 - o Ou d'un compte machine dans l'AD
 - o Ou à défaut par adresse MAC
- Les adresses IP et VLAN sont fixées par le CHU
- Les équipements ne seront connectés que s'ils respectent les règles élémentaires de sécurité : mises à jour, version supportée, antivirus
- La disponibilité en prise réseau doit être étudiée en amont
- Les autorisations d'accès extérieur devront être validées avant d'être envisagées

D. FOURNITURE DE POSTES CLIENTS

- Les postes clients sont préférentiellement fournis par le CHU

- A défaut, les postes devront respecter les règles élémentaires de sécurité : mises à jour, version supportée, antivirus
- Ils devront être inclus au domaine CHU pour gestion centralisée
- Les versions système et les logiciels utilisés devront être validés

E. APPLICATIONS CLIENTS LOURDS

- Les logiciels doivent être référencés par la direction informatique
- Les installations sont à fournir sous forme de .MSI pour être distribuables

F. APPLICATIONS WEB

- Les navigateurs validés sont Firefox et Chrome
- Pour des raisons de sécurité, Internet Explorer n'est plus supporté
- L'application doit respecter les standards et n'utiliser que le protocole https

G. SAUVEGARDE

Un descriptif détaillé des données à sauvegarder est attendu (emplacement et périodicité) pour minimiser le risque de perte de données avec éventuellement les scripts qui permettront ces sauvegardes s'il y a lieu. L'intégration à l'outil de sauvegarde du CHU, VEEAM, est préconisée, à défaut le prestataire engage sa responsabilité sur la mise en place et le suivi des sauvegardes

Modalités de mise en œuvre de la Télémaintenance

1. Contrat de travail des intervenants:

Les contrats de travail des professionnels susceptibles d'effectuer de la télémaintenance doivent contenir une clause relative au secret médical et à la confidentialité des données.

2. Clauses de confidentialité :

Les supports informatiques fournis par le Centre Hospitalier à la société prestataire de service de télémaintenance restent la propriété du Centre Hospitalier.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont la société prestataire de service de télémaintenance prend connaissance à l'occasion de l'exécution des interventions de télémaintenance.

Conformément à l'article 29 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la société prestataire de service de télémaintenance s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées, ou communiquées à des personnes non autorisées

La société prestataire de service de télémaintenance s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel :

- 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 pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent 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 permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat;
- Prendre toutes mesures de sécurité, notamment matérielle, pour assurer la conservation et l'intégrité des documents et informations traitées pendant la durée du présent contrat;
- Et en fin de contrat à procéder à la destruction de tous les fichiers manuels ou informatisés stockant les informations saisies.

A ce titre, la société prestataire de service de télémaintenance ne pourra sous traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable du Centre Hospitalier.

Le Centre Hospitalier se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par la société prestataire de service de télémaintenance.

En cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du nouveau code pénal.

Le centre hospitalier pourra prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non respect des dispositions précitées.

3. formation et sensibilisation des acteurs :

Les salariés de la société prestataire de service de télémaintenance qui réalisent des opérations de télémaintenance doivent être formés à la confidentialité des données personnelles à leur non divulgation et à leur destruction et non conservation ainsi qu'au secret professionnel.

4. Données anonymisées :

la société prestataire de service de télémaintenance s'assure que les données sortantes destinées à la réalisation de la télémaintenance seront destinées uniquement à cet usage et seront anonymisées, sauf si les données sont strictement nécessaires à l'exécution de la prestation.

5. Accès aux dispositifs :

L'accès aux équipements est réalisé en accord avec le Centre Hospitalier selon des plages horaires définies pour éviter d'intervenir pendant l'utilisation du dispositif médical.

Un référent du Centre Hospitalier sera présent auprès du dispositif médical lors des interventions en télémaintenance.

6. Equipements concernés et types d'actions autorisées :

Une annexe comprenant la liste des équipements concernés par la télémaintenance avec la liste des actions autorisées ou non, le protocole d'accès ainsi que les ports à utiliser est joint au contrat de télémaintenance.

Toutes les actions déclanchant

- une action du dispositif,
- une modification de l'interface utilisateur,
- un ajout d'une fonctionnalité,

Ainsi que les mises à jours logiciels sont interdites par télémaintenance.

7. compte rendu d'intervention et traçabilité des actions :

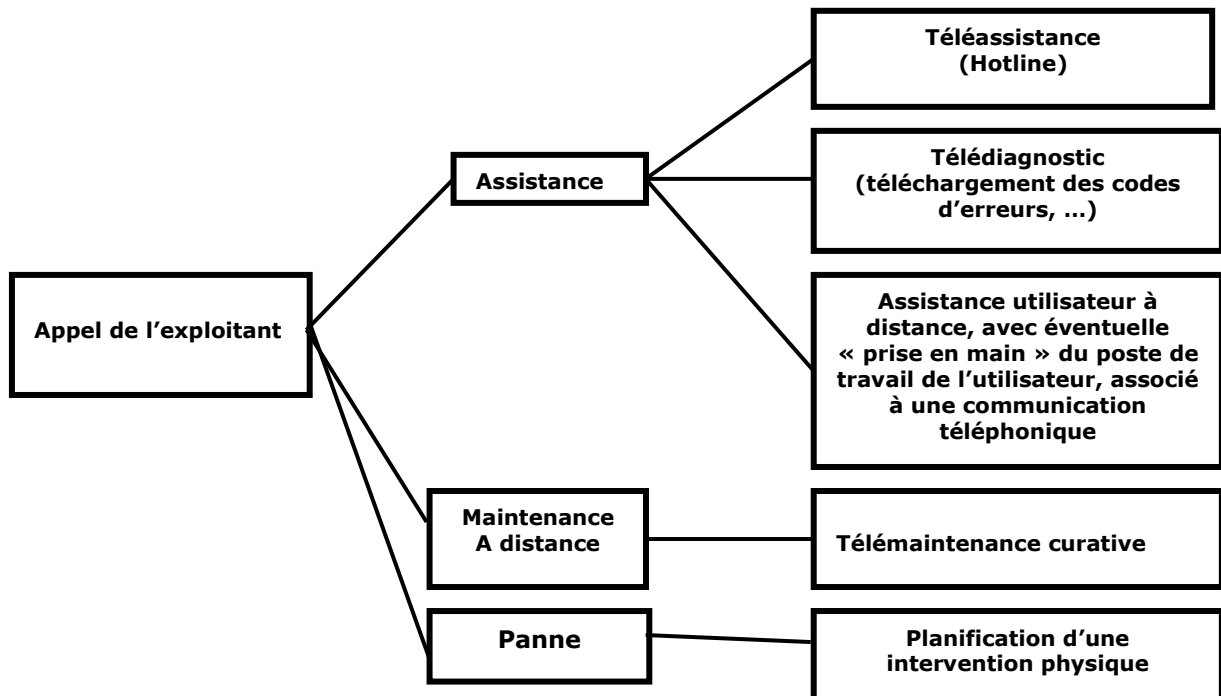
Chaque opération de maintenance fera l'objet d'un descriptif précisant les dates, la nature des opérations et les noms des intervenants. Il sera transmis au Centre Hospitalier.

En cas de télémaintenance permettant un accès à distance aux fichiers du Centre Hospitalier, la société prestataire de service effectuant la télémaintenance prend toutes dispositions afin de permettre au Centre Hospitalier d'identifier la provenance de chaque intervention extérieure. A cette fin, la société prestataire de service de télémaintenance s'engage à obtenir l'accord préalable du Centre Hospitalier avant chaque opération de télémaintenance dont elle prend l'initiative.

Des registres sont établis sous les responsabilités respectives du Centre Hospitalier et de la société prestataire de service de télémaintenance mentionnant les « date » et « nature » détaillées des interventions de télémaintenance ainsi que les noms de leurs auteurs.

8. logigrammes décisionnels :

8.1 Intervention effectuée à la demande du Centre hospitalier :



8.2 Intervention sans sollicitation de l'exploitant :

Seuls la télésurveillance et le déploiement de patch touchant exclusivement les applications de la société prestataire de service de télémaintenance peuvent être déployés sans demande de l'exploitant.