

Annexe - Politique informatique du CHU de Tours

	Nom	Date	Commentaire
Rédacteur	PROVOT Didier	11/02/2015	Reprise de la version précédente avec remise en forme, modifications et ajout de nouveaux thèmes
Vérificateur 1	LAUNAY Philippe	12/02/2015	
Vérificateur 2			
Vérificateur 3			
Mise à jour	PROVOT Didier	12/02/2015	Ajout recommandations ASIP pour la télémaintenance
Mise à jour	BOISMARD Philippe	16/02/2015	Précision antivirus réseau page 8
Mise à jour	PROVOT Didier	17/02/2015	Remise en page de la page 8
Mise à jour	PROVOT Didier	18/03/2015	Modifications suite aux remarques de Patrick
Mise à jour	LAUNAY Philippe	19/03/2015	Ajustement architecture Oracle
Mise à jour	BOISMARD Philippe	23/03/2015	Ajout des paragraphes « intersite » et « sécurité »
Mise à jour	DONDOSSOLA R.	12/08/2015	Précision sur les OS interdits au CHU.
Mise à jour	BOISMARD	12/10/2015	Précision WIFI et protection antivirale des Dispo. Connectés
Mise à jour	DONDOSSOLA R.	30/10/2015	Diverses corrections particulièrement partie vmware et OS
Mise à jour	LAUNAY Philippe	28/01/2016	Suppression référence Time Navigator
Mise à jour	LAUNAY Philippe	05/02/2016	Refonte pré requis candidat
Mise à jour	LAUNAY Philippe	02/03/2016	SCCM Adminstudio
Mise à jour	BOISMARD Philippe	07/04/2016	Hébergement Millenium / Carestream ajout 1.8.6
Mise à jour	BOISMARD Philippe	02/03/2017	Actualisation WIFI(1.8.2) et Télémaintenance (2.1)
Mise à jour	PROVOT Didier	16/05/2017	Actualisation de l'OS des postes de travail
Mise à jour	PROVOT Didier	30/05/2017	Suppression de la partie poste de travail Windows XP
Mise à jour	DONDOSSOLA R.	14/08/2017	v21 – ajout Unity + vmware + bl460c Gen9
Mise à jour	LAUNAY Philippe.	03/04/2018	Prise en compte architecture SQL Server
Mise à jour	LAUNAY Philippe.	20/06/2019	Actualisation
Mise à jour	GENESTAL Erwan	20/06/2019	Ajout du NAC et corrections réseau
Mise à jour	DONDOSSOLA R.	25/06/2019	Corrections partie système, stockage, OS, virtu, Citrix...
Mise à jour	LAUNAY Philippe	31/12/2019	Mise à jour SGBD
Mise à jour	MONTASSIER G.	08/10/2020	Mise à jour frontend
Mise à jour	GENESTAL Erwan	30/04/2021	Mise à jour infra réseau
Mise à jour	LAUNAY Philippe	03/05/2021	Mise à jour infra SGBD Oracle
Mise à jour	MONTASSIER G.	11/05/2021	Mise à jour frontend
Mise à jour	Mise à jour	23/03/2023	Mise à jour infra réseau
Mise à jour	PLY	23/03/2023	Mise à jour infra SGBD
Mise à jour	GENESTAL Erwan	23/05/2023	Mise à jour des annexes relatives à la PGSSI-S
Mise à jour	GENESTAL Erwan	15/09/2025	Mise à jour infra réseau

PLAN :

1. ARCHITECTURE	4
1.1 TOPOLOGIE	4
1.2 SYSTEMES.....	4
1.3 STOCKAGE	4
1.4 SYSTEMES D'EXPLOITATION	4
1.5 VIRTUALISATION	4
1.6 ARCHITECTURE CITRIX	5
1.7 BASES DE DONNEES	5
1.8 RESEAU	7
1.9 POSTES DE TRAVAIL	10
2. EXPLOITATION ET MAINTENANCE.....	12
2.1 TELEMANTENANCE.	12
2.2 SYSTEME.	12
2.3 RESEAU	12
2.4 SUPERVISION	12
3. SECURITE.....	13
3.1 SECURITE DES ACCES.....	13
3.2 SAUVEGARDES.....	13
3.3 ANTIVIRUS.....	13
4. SYNTHESE DES PRECONISATIONS D'INFRASTRUCTURE	14
5. ELEMENTS A FOURNIR PAR LE CANDIDAT.....	15
5.1 SERVEURS.....	15
5.2 STOCKAGE	15
5.3 RESEAU	15
5.4 POSTE DE TRAVAIL	15
5.5 VIRTUALISATION	15
5.6 ORACLE /SQL SERVER	15
5.7 SECURITE DES DISPOSITIFS CONNECTES	17
5.8 CADRE DE REPONSE OBLIGATOIRE.....	17

Usage du document : ce document est présenté sous sa forme la plus détaillée. Suivant le cahier des charges et la pertinence ou non par rapport à la procédure, il est possible de le simplifier en supprimant des paragraphes et des informations mais sans en modifier l'esprit ou de le mettre en annexe en ne gardant que la synthèse.

Pour les cahiers des charges les plus simples, le minimum obligatoire est le chapitre « Synthèse des préconisations d'infrastructure »

Les annexes sont des documents à la disposition des candidats en téléchargement sur le site [PGSSI-S | Agence du Numérique en Santé \(esante.gouv.fr\)](https://esante.gouv.fr). Pour les cahiers des charges les plus importants, ils peuvent être intéressants pour sensibiliser certains candidats qui les ignorent.

Préambule pour le candidat : en cas d'incompatibilité de la solution proposée avec les attentes du CHRU de Tours, les écarts seront clairement indiqués et une solution alternative sera soumise à l'approbation du CHRU de Tours. Dans tous les cas, le candidat devra décrire la solution technique permettant de valider ou non l'adéquation aux prérequis décrits ci-dessous

1. Architecture

1.1 Topologie

Aujourd'hui le CHRU met en place une politique de consolidation de son architecture afin d'éviter toute disparité dans les types de matériels, systèmes d'exploitation et système de gestion des bases de données. Le CHRU dispose historiquement de deux salles serveur sur le site de Bretonneau. Depuis 2021, un datacenter a été créé sur le site de Trousseau distant de 10 Km. Les nouveaux équipements en haute disponibilités sont ainsi répartis entre ces deux sites.

1.2 Systèmes

Pour la production, l'architecture système est composée de 2 châssis C7000 dotés de la Technologie Virtual Connect, eux-mêmes constitués de serveurs type lame BL460c Gen9 Bi-pro. Ces châssis sont répartis entre les 2 salles machines (B01 et B54) du campus de Bretonneau distantes de 700m longueur fibre.

Pour la préproduction l'architecture est également composée de 2 autres châssis C7000 répartis entre les 2 mêmes salles de production, et équipés de lames BL460c.

La nouvelle architecture est composée de :

- Dell PowerEdge R6515 pour les bases Oracle consolidées
- Dell PowerEdge R7515 pour les machines virtuelles

Cette nouvelle infrastructure sera répartie entre les salles de Bretonneau (B01) et Trousseau (T24)

1.3 Stockage

Pour la production ainsi que la préproduction, le stockage est composé de deux baies EMC Unity XT680 dans chacune des salles de production de Bretonneau, en backup l'une de l'autre. La virtualisation du stockage est assurée par des clusters VPLEX, assurant la haute disponibilité. Des clusters de VM délivrent les services NFS et CIFS et assurent la HA au niveau files. Un 3^{ème} site équipé d'une VNX 5100 permet d'héberger les VM d'arbitrage de l'ensemble des dispositifs en haute disponibilité.

1.4 Systèmes d'exploitation

Le CHRU gère trois types de système d'exploitation :

- Windows : la logique est d'implémenter sur la version de Windows Server la plus à jour, en version 64bit. L'implémentation des versions de Windows non supportées par Microsoft à la date de parution de l'offre, c.-à-d. Windows NT, 2000, 2003 et 2008 est strictement interdite.
- Linux : Le CHRU installe actuellement la distribution RedHat Enterprise 64 bits 6.x ou 7x. Le CHRU n'implémente pas les distributions tierces comme Suse, Debian, Centos, Fedora et autres.
- Oracle Linux : Cette distribution est installée en 64 bits pour la gestion de bases Oracle

1.5 Virtualisation

Hormis pour les produits Oracle, la politique du CHRU de Tours est d'installer les systèmes sur des Machines Virtuelles VMware.

Les systèmes installés sur ces serveurs sont des hyperviseurs Vsphere ESXi Enterprise version 6.5.

Pour la production, la répartition actuelle de l'architecture est constituée de serveurs HP BL460c Gen9 sous Vshpere ESXi Enterprise dans chacune des 2 salles machines (B01 et B54). La haute disponibilité est donc assurée simultanément en local et à distance en cas de désastre d'une salle. Les datastores de production sont des luns en réplication synchrone entre les 2 salles. Tous les datastores sont des distributed devices VPLEX en Cross Connect.

2 Clusters de 2 nœuds sont également mis en place sur des sites distants :

- 2 DL360p Gen8 à la Blanchisserie
- 2 DL380p Gen8 sur Trousseau

Pour la pré-production, la répartition actuelle de l'architecture est également constituée de lames HP BL460c sous Vshpere ESXi Enterprise.

1.6 Architecture Citrix

Le CHRU est pourvu d'une ferme Citrix installée sur l'architecture de virtualisation Vmware décrite ci-dessus. Cette ferme est en version 7.15 et publie principalement les applications Evluance (éditeur MainCare) pour la gestion administrative du patient, la gestion économique et financière de l'établissement, la gestion des ressources humaines et d'autres applications.

1.7 Bases de données

1.7.1 Architecture des applications

Le CHRU a pour politique la mise en œuvre d'architecture 3 tiers (séparation des données de base par rapport aux progiciels applicatifs). La partie applicative est de préférence hébergée par des machines virtuelles. La partie donnée, dans le cas de bases de données ORACLE est hébergée sur des clusters dédiés ne contenant aucun programme éditeurs

1.7.2 Architecture bases de données ORACLE

Le CHRU privilégie les bases de données ORACLE. A ce jour, dans le cadre de sa politique de sécurité, l'architecture mise en place par le CHRU est la suivante

- 19C patch 10 (à la date de rédaction du présent CCTP). En cours migration 19c patch 18
- Mise en œuvre architecture RAC
- Stockage de type ASM (réplication assurée par VPLEX)
- Insertion et monitoring des bases dans l'outil Cloud Control 13c du CHRU
- La production est assurée par quatre clusters ORACLE RAC en stockage ASM
- Supervision avec l'outil Cloud Control V13

Le Titulaire devra spécifier le type et la version de sa base de données. Il devra aussi préciser les volumétries initiales des bases, ainsi que les taux prévisionnels d'accroissement ou les formules permettant de le calculer. Les stratégies rman et datapump des bases sont à préciser avec les rétentions sur disque (ainsi que la volumétrie générée). Les mécanismes de sécurisations supportés et privilégiés devront être explicitement décrits (Dataguard, RAC, ...).

1.7.3 Architecture bases de données SQL Server

Le CHRU exploite également une architecture consolidée pour les bases de données SQL Server permettant une haute disponibilité pour les bases hébergées sur ces instances

Cette architecture consolidée est composée d'un cluster composé de 2 nœuds à la date de rédaction du présent CCTP). Il héberge le moteur SQL Serveur 2017 permettant d'assurer la compatibilité des instances de 2008 à 2017

L'ensemble des procédures d'exploitation sont prises en charge par les procédures standards mises en place au CHRU (sauvegardes, rebuild des index, ...)

Toute base SQL Server devra s'intégrer à cette architecture. Le Titulaire devra spécifier le type et la version de sa base de données. Il devra aussi préciser les volumétries initiales des bases, ainsi que les taux prévisionnels d'accroissement ou les formules permettant de le calculer. L'ensemble de ces informations sera recueilli par un formulaire fourni par le CHRU de Tours et rempli par le Titulaire

Dans l'hypothèse où un éditeur ne souhaiterait pas intégrer sa ou ses bases SQL Server sur l'une des architectures consolidées, le CHRU de Tours ne traitera pas celles-ci comme bases de données SQL Server mais comme une application. En conséquence, les tâches de sauvegarde et d'exploitation des bases seront à la charge et sous la responsabilité de l'éditeur. Il devra, de plus, faire la preuve de leurs mises en œuvre avant passage en production.

Les fichiers résultant des dumps réalisés par les procédures de l'éditeur seront récupérés lors de la sauvegarde quotidienne du serveur via l'outil AVAMAR

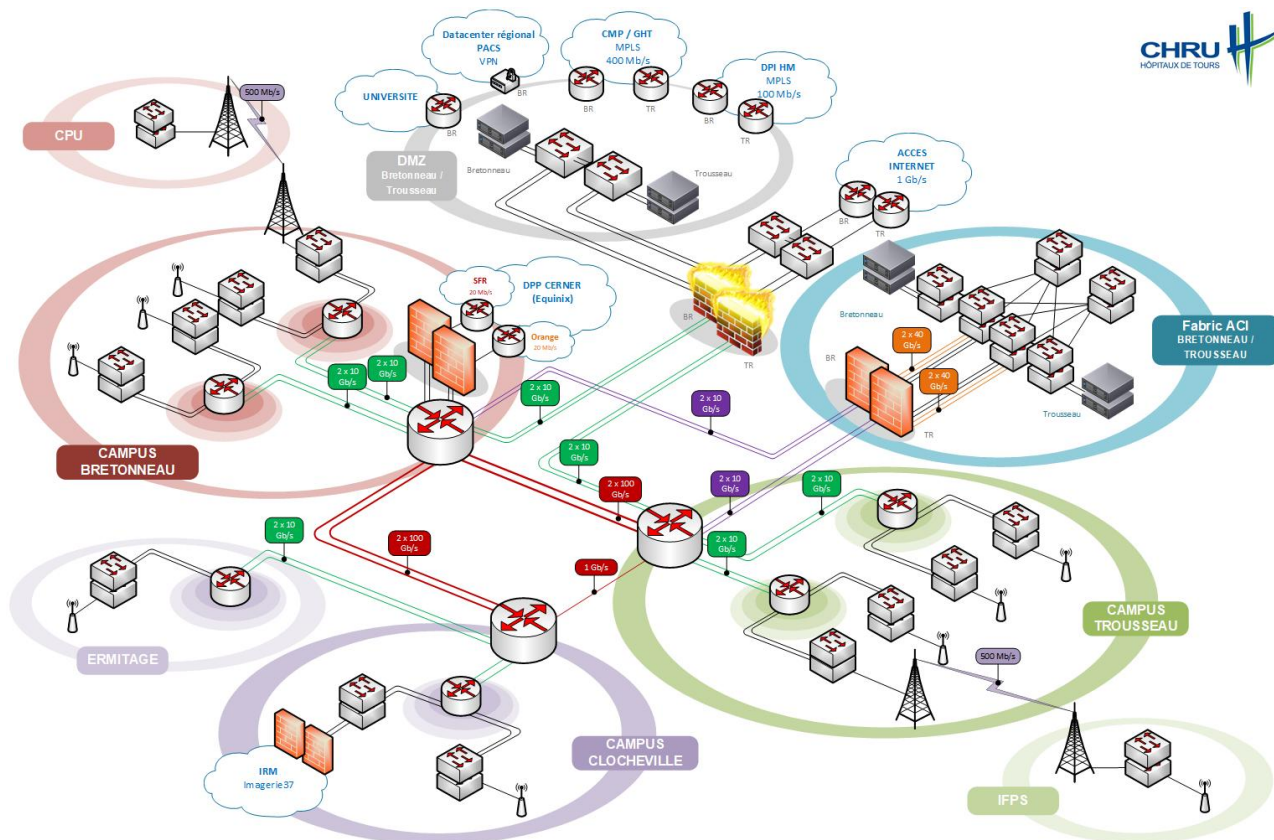
1.7.4 Autres SGBD

Dans le cas où le type de base de données n'est pas Oracle ou SQL Server ou que la base de données n'intègre pas nos pré requis technique dont la consolidation, la supervision, l'administration, la maintenance corrective et évolutive (changement de version) devront être assurés par le Titulaire par le biais de la solution de télémaintenance proposée par le CHRU.

Le CHRU de Tours ne traitera pas ces bases en tant que bases de données SQL mais comme une application. En conséquence, les tâches de sauvegarde et d'exploitation des bases seront à la charge et sous la responsabilité de l'éditeur. Il devra, de plus, faire la preuve de leurs mises en œuvre avant passage en production.

1.8 Réseau

1.8.1 Schéma d'architecture simplifié



1.8.2 Cœur de campus

Le cœur de campus de chaque site (Trousseau / Bretonneau / Clocheville) est composé de switch niveau 3 Cisco Catalyst 9500 en mode VSL (virtual stackwise). Sur Bretonneau ils sont situés chacun dans chacune des deux salles informatiques (B01 et B54). Sur Clocheville et Trousseau ils sont situés dans la même salle serveur. Avec la construction du Nouvel Hôpital Trousseau, les cœurs de Campus de Trousseau seront également répartis dans deux locaux distincts.

1.8.3 Pied de bâtiments

La plupart des bâtiments des 4 principaux sites du CHRU (Trousseau / Bretonneau / Clocheville / Ermitage) dispose d'un local appelé répartiteur général (RG) qui abrite le pied de bâtiments constitué de deux switchs niveaux 3 Cisco Catalyst 4500x en VSS ou de Catalyst 9500 en VSL. Les 4500x sont rattachés aux cœurs de campus via deux liens fibre 10 Gb/s et les 9500 en 50 Gb/s.

1.8.4 Distribution

Pour la distribution les accès se font sur des piles de switchs Cisco C9200L ou C2960X rattachées en double attachement 2 x 1 Gb/s ou 2 x 10 Gb/s sur les deux châssis pieds de bâtiment (C4500-X VSS ou C9500X selon la taille des bâtiments).

Dans le cas où le projet concerne la connexion d'appareils biomédicaux connectés le candidat devra se conformer aux recommandations de l'ASIP décrites dans le « Guide Pratique Règles pour les dispositifs connectés d'un Système d'Information de Santé ». (Voir extrait en annexe 1)

1.8.1 Réseaux de datacenter

La connexion des serveurs se fait au travers d'une infrastructure de type fabric ACI de Cisco répartie entre les sites de Bretonneau et Trousseau (liaison niveau 2). Les flux entrants et sortants des réseaux de datacenter sont filtrés par des firewalls Palo Alto placés en coupure via deux liens 10 Gb/s.

1.8.2 Equipements Wifi

Le CHRU dispose d'un réseau Wifi répondant aux normes 802.11n (2,4 / 5 / 6 Ghz) composé de bornes C2702I-E, C2802I-E C9164-I-E gérées par deux contrôleurs Cisco répartis entre Trousseau et Bretonneau.

Actuellement seuls les bâtiments accueillant du soin et des services tertiaires sous couverts. L'accroissement de la couverture est en cours pour atteindre une couverture totale en 2029 (tous bâtiments et tous étages).

Dans le cas où le projet à mettre en place nécessite des accès sans fil, le candidat devra utiliser le réseau mis en place par le CHRU.

En tout état de cause le candidat devra se conformer aux recommandations de l'ASIP décrites dans le « Guide pratique spécifique pour la mise en place d'un accès Wifi ». (Voir extrait en annexe 2)

1.8.3 Authentification (NAC)

Le CHRU dispose d'un mécanisme d'authentification (NAC : Network Access Control) des équipements connectés au réseau. Il permet de n'autoriser la communication que si l'équipement est reconnu selon différents critères (appartenance au domaine, présence d'un certificat, adresse mac autorisée...). L'équipement devra dans la mesure du possible implémenter le protocole 802.1x pour valider cette authentification.

1.8.4 Câblage

Le CHRU délègue ses travaux de câblage à la société EIFFAGE. Le câblage est réalisé en catégorie 6A minimum.

Le candidat peut estimer nécessaire d'effectuer des câblages (cuivre ou optique). Il s'appuiera de préférence directement sur la société titulaire de ce marché au CHRU lors des travaux, ou effectuera ces travaux par ses propres ressources en s'engageant à respecter la charte de câblage remise à sa demande.

Les liaisons en fibres optiques sont de type multimode au sein d'un bâtiment et en monomode pour les liaisons inter-bâtiments/longues distances.

1.8.5 Liaisons intersites

Les 3 campus (Trousseau, Bretonneau, Clocheville) sont interconnectés entre eux via des fibres noires en 2 x 100 Gb/s. Des multiplexeurs/démultiplexeurs (DWDM) sont placés à chaque extrémité pour multiplier les capacités d'interconnexion entre Trousseau et Bretonneau.

L'EPHAD L'Ermitage est raccordé à Clocheville via deux fibres noires en 2 x 10 Gb/s. La clinique psychiatrique universitaire (CPU) et l'institut de formations aux professions de santé (IFPS) sont reliés respectivement à Bretonneau et Trousseau via des faisceaux hertziens à 500 Mb/s.

Les autres sites du CHRU sont interconnectés via un réseau MPLS géré par un opérateur délégataire. Selon la taille du site les débits varient entre 4 Mb/s et 100 Mb/s.

1.8.6 Accès Internet

L'accès Internet principal du CHRU est constitué de deux liens opérateur redondants à 1 Gb/s, l'un arrivant sur le site de Bretonneau et l'autre sur le site de Trousseau.

En outre des accès Internet de type FTTH sont déployés pour des besoins spécifiques et lorsque l'accès Internet doit être dissocié de la sortie principale.

1.8.7 Sécurité des flux externes

La protection des accès vis-à-vis d'Internet est obtenue par une plateforme Checkpoint HA offrant les principales briques nécessaires à sa sécurité IPS, filtrage URL, contrôle des accès, IPSec-VPN, antivirus WEB. Les fonctions antivirales de messageries sont effectuées par la solution HA IMSVA de TREND. Les flux SSL sont soumis à un décryptage et une analyse antivirus en dehors des exceptions légales.

1.8.1 Sécurité des flux internes

Les flux internes suivants sont filtrés par des firewalls Palo Alto :

- Flux entrants du datacenter
- Flux sortants du datacenter
- Flux entre la VRF biomed et la VRF bureautique
- Flux entre catégories de réseaux de serveurs

1.8.2 Hébergement des applications Dossier Patient MILLENNIUM (CERNER) et des archives des modalités d'imagerie PACS

Le Dossier Patient MILLENNIUM de l'éditeur CERNER est hébergé par la société EQUINNIX. Les accès à l'application depuis le CHRU de Tours se font au travers de deux liens de 100 Mbps, en « mulihoming » (Orange/SFR) au travers de deux pare feux Checkpoint dédiés à cet hébergement. Les firewalls sont gérés par les équipes du CHRU de Tours et les abonnements opérateurs fournis par CERNER. CERNER assure le cryptage de ces flux de données sur le réseau public au travers d'une liaison site à site entre les routeurs BGP4 du CHRU et ceux de l'hébergeur.

Le PACS MIRC de PHILIPPS est accessible en local sur un serveur local CESAP fourni par l'éditeur PHILIPPS pour les examens récents (2 années). Au-delà les examens sont transférés chez l'éditeur PHILIPPS qui en assure le stockage et l'archivage, Ce transfert s'effectue via le lien internet mutualisé du CHRU de Tours au travers de deux boîtiers SRSA situés en DMZ(répartis entre Trousseau et Bretonneau) fournis et opérés par l'éditeur. Les examens récents sont donc consultés en local, et les plus anciens accessibles via le boîtier SRSA sur les serveurs de l'éditeur.

Les données transitant entre le boîtier SRSA et les sites publics de PHILIPPS sont cryptées par l'éditeur.

1.9 Postes de travail

1.9.1 Les micro-ordinateurs

Le parc est constitué de micro-ordinateurs âgés de 0 à 6 ans. Les configurations matérielles les plus basses sont des matériels équipés de micro-processeurs Celeron avec 1 Go de RAM et 300 Go d'espace disque. Chaque poste est issu d'un disque maître en Windows 7 64 bits ou Windows 10 (depuis la version 1804 jusqu'à dernière version).

Tous les postes et les imprimantes sont en DHCP.

Certains logiciels sont installés de base :

Sur le système d'exploitation Windows 7 ou 10 :

- Pack Office 2010
- Acrobat reader 11
- Internet Explorer 11 (éventuellement Firefox version 74.0.1 ou Edge Chromium version 85.0.564.68)
- Client Citrix 12.3
- Java 1.6.27
- Framework 4

Dans la mesure où cela est possible le candidat s'appuiera sur la configuration des postes de travail présentée ci-dessus et privilégiera la version 10 de Microsoft Windows.

1.9.2 Les postes légers mobiles

Le CHRU a équipé ses services de soins de clients légers mobiles. Ces matériels sont connectés actuellement en Wifi sur l'application dossier patient par l'intermédiaire d'un client Citrix.

Le candidat pourra éventuellement rendre son application accessible sur ces matériels au travers d'une page Web ou du client Citrix après une étude de faisabilité (compatibilité, volumétrie des échanges, authentification, etc ...) Toute installation d'un réseau Wifi distinct, dédié, sera soumise à l'approbation de la DSI du CHRU de Tours, le CHRU se réservant le droit d'imposer les bandes de fréquences autorisées.

1.9.3 Les imprimantes

Les imprimantes sont essentiellement des imprimantes laser noir et blanc installées en réseau. Des serveurs d'impressions sont en cours de déploiement mais pas de généralisation pour le moment.

Les postes sont en DHCP.

1.9.4 La télédistribution

La télédistribution sur les postes Windows se fait via la plate-forme SCCM. Cette plateforme permet la distribution de « packages » réalisés par l'outil ADMINSTUDIO.

Aucune installation manuelle d'application hors package SCCM n'est prévue

En conséquence, le titulaire s'engage donc fournir

- Les sources nécessaires à l'application (de préférence MSI)
- La documentation d'installation associée
- La liste des prérequis nécessaires à son utilisation
- Si besoin, les sources et documentation des prérequis
- Une assistance sur place ou à distance permettant la réalisation du package applicatif
- Une procédure ou une assistance permettant la validation du package réalisé

De plus, lors de l'évolution du produit (changement de version ou autres), le titulaire s'engage à en informer le Département Technique et de fournir tous les éléments décrits ci-dessus permettant la prise en charge de cette évolution

2. Exploitation et Maintenance

2.1 Télémaintenance.

Le titulaire s'engage à n'utiliser que les outils de télémaintenance (portail Wallix) mis à disposition par les équipes de la Direction du Système d'Information, respectant ainsi la politique de sécurité mise en œuvre par l'institution (sécurité antivirale, cryptage, confidentialité, traçabilité). Ces outils donnent l'accès aux ressources internes de type Microsoft ou Posix.

Les transferts de fichiers peuvent être assurés via un serveur FTP sécurisé (FTPs) en DMZ, sous réserve de limitations en volume et en durée de stockage.

La mise en œuvre de tunnel SSL crypté, entre le siège du titulaire et les équipements dont il a charge de maintenance dans l'établissement, n'est autorisée que si le CHRU de Tours peut en assurer le déchiffrement (analyse comportementale et antivirale).

En tout état de cause le candidat devra se conformer aux recommandations de l'ASIP décrites dans le guide des « Règles pour les interventions à distance sur les systèmes d'information de santé ». (Voir extrait en annexe 3)

2.2 Système.

Le CHRU adhère au marché UNIHA pour la partie maintenance de serveurs, de baies de stockage et de bibliothèques de backup. Les nouveaux éléments acquis sont sous garantie constructeur initiale. A la sortie de celle-ci, la politique du CHRU est d'intégrer les éléments aux contrats de maintenance UNIHA (marchés détenus aujourd'hui par BULL) plutôt que de renouveler la maintenance constructeur. Différents types de SLA sont envisageables selon la criticité des serveurs et le type d'architecture.

2.3 Réseau

Le CHRU adhère au marché UNIHA pour la partie maintenance des équipements constituant son réseau. Cette maintenance garantit, en cas de dysfonctionnement, un retour en fonctionnement normal de 12H heures ouvrées. Ce délai est acceptable dans la mesure où chaque équipement sensible, s'il n'est pas doublé, peut disposer de deux cartes réseau raccordées à deux équipements distincts.

Sur qualification particulière d'application sensible, après accord de la DSI, cette GTR peut être ramenée à 4H.

2.4 Supervision

La supervision des équipements réseau et de certains serveurs est assurée par une plateforme de supervision NAGIOS. Le CHRU est en cours de mise en place de l'outil SCOM qui permettra de superviser l'ensemble des serveurs sous système d'exploitation WINDOWS :

- Soit c'est le CHRU qui assure cette supervision par le biais d'outils existants et qui, pour certains, ouvre les appels chez les mainteneurs
- Soit cette supervision est assurée par le Titulaire, par le biais de connexion authentifiée conforme à la politique de sécurité du CHRU et validée par la DSI entre le CHRU et le site du candidat.

La supervision des bases de données ORACLE est assurée via l'outil GRID CONTROL 12c implémenté au CHRU. D'autre part, le CHRU dispose d'une assistance extérieure (société DIGORA) pour la supervision de bases de données ORACLE à condition que celles-ci intègrent l'architecture cluster RAC 11.2.0.4 décrite ci-dessus.

3. Sécurité

3.1 Sécurité des accès

La politique du CHRU est d'intégrer l'ensemble des serveurs et des postes de travail dans l'Active Directory. Tous les postes de travail se connectent au domaine Active Directory en respectant la politique de sécurité mise en place ; le mot de passe doit comporter un minimum de 8 caractères composés de 3 types (Majuscule, minuscule, numérique) ; lors du changement de mot de passe le nouveau doit être différent des 3 derniers déjà utilisés.

3.2 Sauvegardes

Le CHRU utilise la solution logicielle AVAMAR société EMC avec des Baies DATADOMAIN pour le stockage des sauvegardes.

Le candidat devra, prévoir une intégration avec la solution AVAMAR/DATADomain

Le Titulaire devra préciser :

- l'emplacement des données à sauvegarder
- les récurrences des sauvegardes
- les durées de rétention
- les commandes à insérer dans les scripts de prétraitement et de post-traitement...
- l'estimation de l'accroissement des volumétries

3.3 Antivirus

Le CHRU dispose de la suite de sécurité de l'éditeur Trend Micro. Notamment :

- La suite Apex One du même éditeur est implémentée sur les serveurs et les postes de travail.
- La solution Deep Security du même éditeur est installée sur tous les serveurs pour le virtual patching. Elle a en plus le rôle d'antivirus sur les serveurs 2003/2008 qui ne sont plus supportés par Apex One.
- Ces solutions sont gérées via une console centrale.
- Ces solutions s'appuient sur des serveurs de sandboxing et de partage des mises à jour / signatures.

Le paramétrage des serveurs, des exclusions de répertoires et des privilèges particuliers (désactivation Real Time Scan...) sont paramétrables via un formulaire spécifique.

Dans le cas où le candidat propose des dispositifs connectés dans son offre, il s'engagera à ce que ses équipements comportent des moyens de sécurité permettant de détecter et de répondre aux menaces liées au codes malveillants. La solution Trend devra être privilégiée.

Dans le cas où le candidat propose une solution différente de celle installée au CHRU, il devra s'assurer de la bonne mise à jour de sa solution et de la remontée en temps réel des alertes.

La solution Checkpoint sécurise la partie accès WEB vers Internet en inspectant les flux.

3.1 EDR

L'EDR Trend Micro Vision One est déployé sur tous les postes et serveurs connectés au réseau. Il permet de collecter de la télémétrie sur l'usage du poste/serveur dans un datalake hébergé en mode cloud. Un moteur de corrélation permet de détecter des signaux faibles et de générer des alertes de sécurité ou de détecter des vulnérabilités de manière proactive.

L'agent permet de faire des actions de remédiations (isolation du poste, déconnexion de l'utilisateur, réinitialisation du mot de passe...) mais n'agit pas sur les fichiers et les processus.

4. Synthèse des préconisations d'infrastructure

En synthèse, les préconisations d'infrastructure du CHRU de TOURS, à la date de rédaction du document, sont:

Back-end

- Mise en œuvre des techniques de Haute Disponibilité
- Architecture 3 tiers (séparation couche applicative, couche base de données, clients)
- Pour la couche applicative, virtualisation sur une architecture VMWARE
 - OS serveurs applicatifs (virtualisé)
 - RHEL 7 ou 6 64 bits
 - WINDOWS 2019, 2016 ou 2012
- Base de données :
 - ORACLE19C patch 10 minimum, gestion ASM, RAC, RMAN pour les sauvegardes, OS ORACLE LINUX 64 bits
 - SQL Server 2017 Always On
- Stockage : Intégration obligatoire au stockage unifié du CHRU de TOURS basé sur deux baies Unity XT680 avec couche VPLEX.
- Archivage : Pas de solution d'archivage
- Sauvegarde : Intégration au logiciel AVAMAR/DATADOMAIN EMC
- Antivirus Deep Security et EDR Vision One de Trend installés sur les serveurs

Front-end

- La compatibilité de l'application avec Windows 10
- Compatibilité de l'application si nécessaire avec Internet Explorer 11 ou Edge Chromium
- Compatibilité de l'application si nécessaire avec Citrix XenApp 7.15
- Antivirus Apex One et EDR Vision One de Trend installés sur les postes de travail
- Annuaire : Conformité avec serveur Active directory 2019 et niveau fonctionnel 2008 R2
- Si la solution nécessite un déploiement de client sur les postes de travail, celui-ci devra impérativement intégrer la plateforme SCCM
-

Réseau

- Wifi : Dans le cas d'utilisation d'équipements mobiles, l'intégration à l'architecture Wifi implantée sur le CHU est obligatoire
- Si l'équipement doit accéder à Internet, il doit être en mesure d'intégrer le certificat SSL du CHRU
- L'équipement ne pourra pas être connecté à la fois sur le réseau du CHRU et à la fois sur un lien communiquant avec l'extérieur (Modem 3G/4G, VPN, lien dédié...)
- Le plan d'adressage sera fourni par le CHU
- L'équipement devra être identifiable via le NAC (Network Access Control) du CHU via le protocole 802.1x notamment

Télémaintenance

- La plateforme sécurisée d'accès à distance pour la télémaintenance est la solution WALLIX
- Les comptes sont désactivés par défaut et ne permettent l'accès aux ressources uniquement dans le périmètre d'intervention
- Les accès sont ouverts à la demande par l'interlocuteur du CHU et pour la durée de l'intervention

5. Eléments à fournir par le candidat

Il est mentionné ci-dessous les marchés d'acquisition contractés par le CHRU. Il est attendu du candidat d'une part qu'il complète si besoin les fournitures nécessaires à son offre et non couvertes par les marchés cités et d'autre part qu'il indique les configurations que le CHRU devra acquérir au travers de ses marchés.

5.1 Serveurs

Le CHRU fait ses acquisitions de serveurs au travers du marché UGAP ou UNIHA.
Le candidat devra donner la configuration la plus exhaustive possible de ses besoins.

5.2 Stockage

Le CHRU a l'obligation d'utiliser le marché UNIHA pour l'acquisition de stockage. Le candidat devra donner la configuration la plus exhaustive possible de ses besoins : volumétries, accroissement et performances, type de stockage, ...

5.3 Réseau

Le CHRU de Tours adhère au segment réseau du marché CAIH. Le constructeur retenu, que ce soit dans le cadre de la rénovation ou de la mise en œuvre de nouvelles structures / bâtiments est Cisco pour la partie switch.

Le candidat devra exprimer ses besoins en nombre de ports, débit par port, degré de sécurisation (agrégations de ports sur deux équipements distincts, teaming actif/passif, actif/actif), besoins en PoE, ...) et approuver l'utilisation du mode de télémaintenance en vigueur au CHRU de Tours.

Une matrice des flux (IP source / IP Destination / Protocole / Port) devra être fournie aussi bien pour la communication en interne (AD, DNS...) qu'en externe.

5.4 Poste de travail

Le CHRU de Tours adhère au segment NTIC UNIHA pour l'acquisition d'ordinateurs, d'écrans, et d'imprimantes.

Le candidat fournira ses prérequis en matière de postes de travail et si besoin de périphériques type lecteurs de badges, douchette codes à barres etc...

Dans la mesure où les prérequis du candidat en termes de postes de travail et de périphériques correspondent à ceux proposés dans le cadre du marché, le matériel sera acquis par cet intermédiaire.

En ce qui concerne les licences Microsoft, le CHRU de Tours adhère au segment NTIC Accord Cadre Microsoft ce qui permet pour un coût annuel par poste, de bénéficier de la quasi-totalité du catalogue de produits Microsoft.

5.5 Virtualisation

Le CHRU adhère au marché UNIHA pour la partie acquisition de licences VMware (via APX).

5.6 Oracle /SQL Server

Le CHRU adhère au marché UNIHA ORACLE et via le CAIH au marché Microsoft.

Il fournira donc les licences Oracle Entreprise et Microsoft SQL Server.

Pour les bases hors Oracle et SQL Server, le candidat devra l'intégrer obligatoirement dans sa proposition les licences.

Pour les bases hors Oracle, le candidat devra intégrer obligatoirement dans sa proposition toutes les prestations liées à la supervision, l'administration, la maintenance corrective et évolutive (changement de version).

5.7 Sécurité des dispositifs connectés

Dans le cas où l'offre comporte des dispositifs connectés, le candidat devra s'engager à respecter les règles de l'ASIP énoncées dans l'annexe 1, en particulier, il indiquera clairement les moyens mis en œuvre pour la protection de ses équipements contre les codes malveillants.

5.8 Cadre de réponse obligatoire

Dans le cas où le candidat met en œuvre et/ou utilise des ressources informatiques dans les domaines suscités il devra impérativement, fournir des réponses explicites sur les éléments exigés par la DSI du CHRU de Tours.

5.8.2 Réseau				
Connectivité réseau cuivre sur équipements CHRU	Nécessité (O/N)	Nombre de ports physiques	Agrégation	PoE
Equipements réseau fourni par le candidat	Switch(1)	Firewall(1)	Adressage privé(1)	Equipement double carte réseau(1)
Télémaintenance	Nécessité (O/N)	Portail SSL du CHRU de Tours	Tunnel site à site	Autre (1)
Connectivité WiFi sur le réseau existant au CHU	Nécessité (O/N)	Bande passante demandée mini/moy/max	QoS demandée	Nécessite un réseau Wifi dédié (1)

(1) Doit être étudié et soumis à l'approbation de la DSI du CHRU de Tours

5.8.7 Sécurité des dispositifs connectés				
	Antivirus	Compatible antivirus CHRU	Si non compatible : éditeur (1)	Autre solution (1)
Poste de travail				
Dispositif connecté				Lu et approuve (2) l'annexe 1 (O/N)

(1) Doit être soumis à l'approbation de la DSI du CHRU de Tours

(2) Le candidat devra expliciter les points sur lesquels il ne peut s'engager

ANNEXE 1

Politique Générale de Sécurité des Systèmes d'Informations de Santé – PGSSI-S publié par l'ANS (Agence du Numérique en Santé)

Le corpus documentaire de la PGSSI-S, Politique Générale de Sécurité des Systèmes d'Information de Santé, offre le cadre de référence nécessaire à la mise en œuvre des règles de sécurité en matière de e-santé.

L'usage du numérique en santé contribue à l'amélioration de la prise en charge du patient. Cependant, face aux menaces engendrées par ces usages, l'Etat a mis en œuvre une politique de gestion des risques.

L'Agence du numérique en Santé (ANS) met en place les cadres de référence pour sécuriser les pratiques en matière de e-santé pour les usagers et les professionnels des secteurs sanitaires.

La Politique Générale de Sécurité des Systèmes d'Information en Santé (PGSSI-S) est un maillon important de cet ensemble normatif.

Ses objectifs :

- Aider les porteurs de projet dans la définition des niveaux de sécurité attendus
- Permettre aux industriels de préciser les niveaux de sécurité de leurs offres
- Soutenir les établissements de santé dans le choix et l'application de leur politique de sécurité

La PGSSI-S s'applique aussi bien au secteur public qu'au secteur privé, aux professionnels de santé, du médico-social et social, aux établissements de soin et aux offreurs de service.

[Fiche thématique de la PGSSI-S](#)

[Corpus documentaire PGSSI-S](#)

ANNEXE 2

Référentiels opposables par arrêté du ministre chargé de la santé

[Référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social \[personnes morales\]](#)

[Référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social \[personnes physiques\]](#)

[Référentiel d'identification électronique des usagers](#)

[Référentiel d'imputabilité](#)

[Référentiel Force Probante des documents de santé](#)

ANNEXE 3

Règles pour les dispositifs connectés d'un Système d'Information de Santé – ASIP Santé PGSSI-S

Deux paliers sont définis pour la mise en œuvre des exigences de sécurité applicables aux dispositifs connectés : un palier intermédiaire (Palier 1), porteur des exigences prioritaires, et un palier supérieur (Palier 2) reprenant les exigences prioritaires et les complétant afin d'offrir un meilleur niveau de sécurité.

Gestion des configurations

N°	Exigence	Niveau d'exigibilité
Gestion des configurations [G]		
[G1]	Le fournisseur et/ou le fabricant doit identifier dans sa documentation (accessible par exemple au travers d'un espace client sur Internet) l'ensemble des composants matériels (serveurs, périphériques, ...) et logiciels (versions des logiciels, systèmes d'exploitation, bases de données, ...) informatiques standards constituant le dispositif connecté ainsi que leurs principales caractéristiques.	Palier 1
[G2]	Le fournisseur et/ou le fabricant doit identifier dans sa documentation l'ensemble des spécifications portant sur le poste d'administration/ utilisation du dispositif connecté (caractéristiques matérielles du poste, version du système d'exploitation, middleware et pilotes, services activés, périphériques, ...).	Palier 1
[G3]	Le système dispositif connecté doit fournir une interface permettant à un système de management des configurations (CMDB) d'un SIS ou à un service de télémaintenance (par exemple pour un Professionnel de Santé en exercice libéral) d'obtenir automatiquement la configuration du système dispositif connecté	Palier 2

Sécurité physique

N°	Exigence	Niveau d'exigibilité
Sécurité physique [S]		
[S1]	Le fournisseur et/ou le fabricant doit identifier dans sa documentation l'ensemble des mesures de sécurité physique (sécurité des locaux, clés du coffret protégeant le dispositif connecté, contraintes d'environnement notamment compatibilité électromagnétique (réseau WiFi, téléphone mobile), sécurité des câblages...) préconisées pour la mise en œuvre du système dispositif connecté au sein du SIS.	Palier 1
[S2]	Le dispositif connecté doit mettre en œuvre des moyens de sécurité physique permettant de détecter toute tentative d'accès physique aux composants internes sensibles (disque dur, interfaces internes, paramétrages matériels par cavaliers par exemple, ...).	Palier 2

Exploitation et communications

N°	Exigence	Niveau d'exigibilité
Exploitation et communications [E]		
Vérification du bon fonctionnement		
[E1]	Les dispositifs connectés doivent disposer d'une fonction permettant de garantir l'intégrité des logiciels et des données sensibles du dispositif au démarrage du dispositif et lors de son fonctionnement. La date de dernière modification des logiciels et des données sensibles dont celles inhérentes à l'appareil est présentée lors de la connexion des utilisateurs.	Palier 1

Mise à jour des dispositifs		
[E2]	Les dispositifs connectés et les logiciels des postes utilisateurs doivent disposer d'une fonction de mise à jour sécurisée des logiciels (logiciels, micrologiciel, ...) permettant de garantir l'origine et l'intégrité des mises à jour.	Palier 1
[E3]	Les dispositifs connectés doivent vérifier la bonne installation d'une mise à jour logicielle avec une possibilité de retour arrière en cas de dysfonctionnement détecté.	Palier 1
[E4]	Les dispositifs connectés et les logiciels des postes utilisateur doivent disposer d'une fonction de mise à jour sécurisée avec notification automatique de l'existence d'une mise à jour des logiciels (logiciels, micrologiciel, ...).	Palier 2
Protection contre les codes malveillants		
[E5]	Les dispositifs connectés doivent comporter des moyens de sécurité permettant de détecter et de répondre aux menaces liées aux codes malveillants notamment dans le cas d'utilisation de supports amovibles. Si le dispositif ne comporte pas de solution de type antivirus l'utilisation de support externe est interdite.	Palier 1
[E6]	Les postes utilisateurs des dispositifs connectés doivent s'adapter ou comporter des moyens de sécurité permettant de détecter et de répondre aux menaces liées aux codes malveillants. Dans ce sens, les logiciels spécifiques à la gestion des dispositifs connectés installés sur les postes utilisateurs sont compatibles avec des solutions de sécurité contre les codes malveillants. Le fabricant doit fournir la liste des outils avec lesquels ses logiciels et matériels sont compatibles.	Palier 1
Sécurité des réseaux		
[E7]	La documentation du dispositif connecté (accessible par exemple au travers d'un espace client sur Internet) doit comporter une matrice des flux réseau (types de protocoles, origine/destination des flux, plan d'adressage...) exhaustive.	Palier 1
[E8]	Les dispositifs connectés doivent comporter des moyens de sécurité permettant de filtrer les données échangées sur les réseaux (types de protocoles, origine/destination des flux, ...).	Palier 2
[E9]	Les postes utilisateurs des dispositifs connectés doivent comporter des moyens de sécurité permettant de filtrer les données échangées sur les réseaux (types de protocoles, origine/destination des flux, ...). Dans ce sens, les logiciels spécifiques à la gestion des dispositifs connectés, installés sur les postes de travail, sont compatibles avec les solutions de sécurité de filtrage réseaux de type firewall personnel.	Palier 1
[E10]	En cas de mise en œuvre de communications sans fil, le dispositif connecté doit être conforme aux exigences en vigueur dans les bonnes pratiques. Concernant le mode WiFi, se référer aux documents de référence dans le domaine.	Palier 1
Sécurité des données		
[E11]	Afin de garantir la confidentialité des données médicales personnelles stockées localement, le dispositif connecté doit embarquer un dispositif de chiffrement des données. Le fournisseur et/ou le fabricant pourra se référer au Référentiel Général de Sécurité (RGS) qui comporte une annexe décrivant les exigences relatives à la fonction de sécurité « confidentialité ».	Palier 2
[E12]	Afin de garantir l'intégrité des données, le dispositif connecté doit mettre en œuvre des protocoles de transmission adaptés permettant de vérifier l'équivalence des données reçues à celles émises.	Palier 1
[E13]	Lors de la numérisation et de la compression des images (imagerie médicale), des procédures normalisées doivent être mises en œuvre afin de garantir l'intégrité de ces données.	Palier 1
[E14]	Les échanges de données du dispositif connecté doivent être conformes aux exigences de sécurité (notamment authentification et chiffrement) identifiées dans le Cadre d'Interopérabilité des SIS publié par l'ASIP Santé.	Palier 1
[E15]	Les échanges de données entre le dispositif connecté et les postes utilisateurs doivent être protégés en confidentialité et intégrité.	Palier 2
[E16]	L'accès aux fonctions d'export de données du dispositif connecté doit être limité à des personnes dûment habilitées.	Palier 1
Gestion des supports amovibles		
[E17]	La fonction de démarrage du dispositif connecté à partir d'un support amovible doit être désactivée en fonctionnement nominal.	Palier 1

Surveillance		
[E18]	Le dispositif connecté doit comporter une fonction d'alerte locale permettant de surveiller le bon fonctionnement, et tout événement pouvant avoir un impact critique sur son fonctionnement.	Palier 1
[E19]	Le dispositif connecté doit comporter une fonction d'alerte s'appuyant sur des mécanismes standards permettant au SIS de surveiller le bon fonctionnement, le contrôle des connexions au dispositif, et tout événement pouvant avoir un impact critique sur son fonctionnement (mise à jour du logiciel, modification de paramètre critiques, ...).	Palier 2
Journalisation		
[E20]	Le dispositif connecté doit comporter une fonction de journalisation locale permettant de conserver une trace des accès au dispositif connecté et de tout événement pouvant avoir un impact critique sur son fonctionnement en particulier les événements identifiés par la règle E18. Le fabricant doit indiquer dans sa documentation les modalités de mise en œuvre de la journalisation en particulier les capacités de stockage de journaux du dispositif connecté et les recommandations en matière de sauvegarde des journaux.	Palier 1
[E21]	Le dispositif connecté doit comporter une fonction de gestion des traces s'appuyant sur des mécanismes standards permettant au SIS de conserver des enregistrements de tout événement pouvant avoir un impact critique sur le fonctionnement du dispositif connecté avec une garantie d'imputabilité pour l'ensemble des opérations effectuées sur ce dispositif. Ces journaux doivent permettre l'analyse ultérieure des causes des dysfonctionnements.	Palier 2
Sauvegardes		
[E22]	Le dispositif connecté doit comporter une fonction de sauvegarde conforme aux exigences en vigueur dans les bonnes pratiques.	Palier 1
Règles de destruction de données lors du transfert de matériels informatiques		
[E23]	Le fournisseur doit mettre en œuvre des fonctions de sécurité d'effacement des données conformes aux exigences en vigueur dans les bonnes pratiques.	Palier 1
Maîtrise des accès [A]		
Contrôle d'accès au réseau		
[A1]	Le dispositif connecté doit comporter une fonction standard d'identification et d'authentification réseau du matériel, par exemple par l'utilisation du protocole 802.1X.	Palier 2
Authentification des utilisateurs		
[A2]	Le dispositif connecté doit comporter une fonction d'authentification des utilisateurs sur la base de comptes nominatifs et au minimum de mots de passe modifiables par les utilisateurs. Les mots de passe par défaut doivent être changés lors de l'installation ou de la première connexion d'un utilisateur et être spécifiques à chaque client.	Palier 1
[A3]	Le dispositif connecté doit comporter une fonction d'authentification forte des utilisateurs pour certains profils (administration, maintenance,...).	Palier 2
[A4]	Le dispositif connecté doit permettre d'imposer une politique de mots de passe (période de renouvellement, règles de constitution des mots de passe, réutilisation d'anciens mots de passe, ...)	Palier 2
[A5]	Tout accès au système dispositif connecté nécessite une authentification préalable.	Palier 1
[A6]	La date de dernière connexion au système dispositif connecté doit être présentée lors de la connexion d'un utilisateur	Palier 1
[A7]	Les logiciels du système dispositif connecté doivent offrir des fonctionnalités de verrouillage automatique en cas d'inactivité prolongée et de blocage de comptes en cas de tentative d'accès non autorisé répétée.	Palier 1
Droits d'accès		
[A8]	Les droits d'accès des utilisateurs doivent être organisés selon des rôles.	Palier 1
[A9]	L'accès aux fonctions de mise à jour des logiciels ou de modification des paramètres sensibles nécessite une authentification forte des utilisateurs. Toute action de validation dans ces contextes nécessite une double confirmation (ex. la validation d'une demande de modification de paramètres sensibles ouvre une fenêtre de dialogue rappelant l'impact d'une telle modification et demandant la confirmation de la demande).	Palier 2

Développement et maintenance des logiciels

N°	Exigence	Niveau d'exigibilité
Développement et maintenance des logiciels [D]		
[D1]	Le fournisseur et/ou le fabricant s'engage à n'installer que les seuls logiciels nécessaires au fonctionnement du dispositif connecté. Le fournisseur et/ou le fabricant s'engage à n'activer que les seuls services nécessaires au fonctionnement du dispositif connecté.	Palier 1
[D2]	L'architecture générale du système dispositif connecté et des logiciels développés doit être sans adhérence avec les briques système standards utilisées, en vue de faciliter les migrations de versions de logiciels. A défaut, le fournisseur doit assurer la compatibilité ascendante avec les évolutions des briques adhérentes.	Palier 1
[D3]	Le processus de développement doit prévoir la gestion des exceptions (débordement de plages de valeurs, erreurs internes des composants, ...).	Palier 1
[D4]	Le fournisseur et/ou le fabricant doit implémenter une fonction permettant de vérifier l'intégrité des logiciels lors de leur démarrage ou lors de leur mise à jour	Palier 1
[D5]	Le fournisseur du dispositif connecté doit assurer un suivi permanent des incidents liés aux dispositifs connectés et met à disposition de ses clients, les correctifs nécessaires. Ce suivi s'inscrit dans le cadre du guide d'organisation de la sécurité de la PGSSI-S.	Palier 1
[D6]	Le fournisseur du dispositif connecté doit assurer un suivi permanent des vulnérabilités liées aux technologies mises en œuvre dans ses produits et met à disposition de ses clients les correctifs nécessaires. Ce suivi s'inscrit dans le cadre du guide d'organisation de la sécurité de la PGSSI-S.	Palier 1
[D7]	Les fonctionnalités de télémaintenance du dispositif connecté doivent être conformes au guide PGSSI-S – Règles pour les interventions à distance sur les SIS.	Palier 1
[D8]	Les modes de tests et de maintenance du dispositif connecté doivent être exclusifs du mode opérationnel.	Palier 1
[D9]	Le dispositif connecté doit disposer d'un mode dégradé (sécurisé) permettant son fonctionnement déconnecté du SIS avec une fonction de reprise des données lors du retour en mode nominal.	Palier 1
[D10]	Le fabricant doit mener des tests de la robustesse des dispositifs connectés (tests aux limites, injection de données malformées, ...)	Palier 1
[D11]	Le fournisseur et/ou le fabricant doit proposer des solutions de restitution des données permettant une reprise de celles-ci par le client notamment en cas de changement d'équipement, dans un format réutilisable par le client.	Palier 1
[D12]	Le fournisseur et/ou le fabricant doit réaliser des tests de non régression à chaque évolution du logiciel ou matériel du dispositif connecté.	Palier 1

Conformité

N°	Exigence	Niveau d'exigibilité
Conformité [C]		
[C1]	Il est du ressort du fournisseur d'acquiescer et de concéder au client l'ensemble des licences d'utilisation nécessaires au fonctionnement du dispositif connecté sauf condition spécifique du client. Ceci concerne les droits d'usage des progiciels, des matériels et de l'ensemble des couches logiques utilisées (Système d'exploitation, algorithmes, progiciels sécuritaires, progiciels réseaux, progiciels de base de données, progiciels systèmes, progiciels de transfert et de prise de main à distance, progiciels applicatifs, etc.).	Palier 1
[C2]	Le fournisseur et/ou le fabricant doit réaliser une analyse de risques du système dispositif connecté et doit adapter les mesures de sécurité à mettre en œuvre dans ses produits au regard des risques résiduels. Il doit informer le client de la méthode d'analyse de risques retenue, des risques couverts et des risques résiduels qui seront portés par le client. Il peut en outre préconiser des mesures de sécurité à	Palier 1

	mettre en œuvre par le client afin de réduire les risques résiduels identifiés dans le cadre des précautions d'usage du dispositif.	
--	---	--