

Exigences sécurité – système d’informations

Le CHU de Bordeaux, ainsi que l’ensemble des établissements de santé au niveau mondial, font face de plus en plus à des attaques informatiques mettant en péril la disponibilité de leurs systèmes d’information, voire même la sécurité des soins de leurs patients.

A ce titre, le CHU de Bordeaux met en œuvre un ensemble de mesures de sécurité sur les systèmes d’informations afin de réduire les risques.

Le CHU de Bordeaux est très attentif aux dispositifs de sécurité informatique disponibles sur les équipements biomédicaux qui sont amenés à être connectés sur son réseau.

1. Déploiement de la solution

1.1 Installation solution logicielle proposée

Le titulaire devra préciser dans sa réponse les licences concédées à l’établissement. Pour chaque logiciel installé, le titulaire devra fournir une description comprenant le type de licence (licence par utilisateur, licence site, licence flottante, abonnement,...).

Le titulaire devra indiquer dans sa réponse les services où programmes qui doivent fonctionner en continue pour la solution logicielle. Le titulaire précisera les services qui seront à superviser par le CHU de Bordeaux pour assurer ce bon fonctionnement.

Déploiement du logiciel

Le titulaire devra préciser dans un schéma l’architecture de son logiciel et fournir ses caractéristiques techniques (client lourd, application web,...).

Pour toute installation de logiciel sur le système d’informations du CHU de Bordeaux, le titulaire devra fournir à la DSIN les sources d’installation du logiciel, le manuel d’installation en français ainsi que le guide d’utilisation en français afin que celui-ci soit validé par les équipes de la DSIN. Le titulaire s’engage à n’installer et à n’activer que les seuls logiciels nécessaires au bon fonctionnement du dispositif objet du marché et après validation par la DSIN de cette installation.

Le déploiement du logiciel sur les postes du CHU de Bordeaux sera assuré par les équipes de la DSIN en lien avec le titulaire.

Précisions sur les données contenues dans la solution logicielle

Le titulaire devra préciser le type de données qui seront enregistrées dans sa solution logicielle et notamment s’il s’agit de données médicales, de production de compte-rendu ou de données administratives. Le titulaire devra indiquer le mode de gestion de ces données (base de données, fichiers plats,...). Dans le cas de données médicales, celle-ci devront être stockés sur un répertoire partagé fourni par la DSIN qui en assure la gestion des sauvegardes et les droits d’accès.

Le titulaire devra indiquer si sa solution nécessite une communication avec l’extérieur de l’établissement.

2. Exploitation de la solution

2.1 Télémaintenance

Le CHU de Bordeaux met à disposition de ses fournisseurs une solution de télémaintenance par bastion. Le titulaire s’engage à utiliser cette solution de télémaintenance. Les outils de télémaintenance type Teamviewer ne sont pas autorisés au CHU de Bordeaux.

Afin de mettre à disposition l’accès par télémaintenance au CHU de Bordeaux, il sera demandé au titulaire de compléter et de signer les documents suivants :

- Convention de télémaintenance EN-SIH-180
- Engagement de confidentialité EN-INF-211
- Engagement du prestataire EN-SIH-263

Un compte de télémaintenance sera fourni à chaque collaborateur du titulaire ayant besoin pour ses fonctions d'accéder au CHU de Bordeaux.

Le titulaire s'engage à fournir un rapport d'intervention après prise de main à distance en précisant les horaires de début et de fin d'intervention.

2.2 Mise à niveau informatique

Le titulaire décrira les mises à niveau inclus dans son offre durant la période de garantie et la période de maintenance. Cela inclus :

- Les mises à jour des logiciels fournis par le titulaire
- Les mises à jour du système d'exploitation des équipements fournis par le titulaire
- Les mises à jour outils de sécurité fournis par le titulaire (antivirus, EDR,...)
- Les mises à jour des interfaces avec le SIH fournis par le titulaire
- Les mises à niveau du matériel (hardware) fourni par le titulaire

Le titulaire décrira les mises à niveau inclus dans son offre pour assurer le maintien en condition de sécurité :

- Les mises à jour de sécurité des outils de sécurité fournis par le titulaire (antivirus, EDR,...)
- Les mises à jour de sécurité du système d'exploitation des équipements fournis par le titulaire

2.3 Maintenance de la solution

Dans le cadre d'une maintenance, le contenu de l'opération devra être fourni au CHU de Bordeaux 10 jours avant l'intervention afin que celle-ci puisse être validée par la DSIN.

Dans le cas d'une mise à jour logicielle, les sources seront à fournir à la DSIN avec la procédure de mise à jour ainsi que la description des nouveautés apportées par la mise à jour.

2.4 Procédure dégradée

Le titulaire devra préciser s'il existe une procédure ou un mode dégradé sur l'équipement permettant de fonctionner en cas de panne d'une ou de toutes les parties du SIH du CHU de Bordeaux. Si cela existe, le titulaire indiquera comment se fait la réconciliation des dossiers créés en mode dégradé.

2.5 Veille sécurité

Le titulaire s'engage à informer le CHU de Bordeaux, via son RSSI (rssi@chu-bordeaux.fr) de toute vulnérabilité, d'incident de sécurité sur la solution et sur son SI d'entreprise qui apparaîtrait durant la phase d'exécution du marché et durant la phase de maintenance.

En cas d'incident de sécurité sur l'équipement du titulaire, celui-ci s'engage à remettre en état le système à ses frais.

Dans le but d'évaluer le bon niveau de sécurité du système, le CHU de Bordeaux pourra réaliser un audit de sécurité lors de la phase de mise en service de la solution et durant la phase d'exploitation. Le titulaire indiquera s'il souhaite être prévenu de ces audits et si oui à quelle échéance. Le compte-rendu de l'audit réalisé sera transmis au titulaire.