1. OBJECTIF DU DOCUMENT

Ce document décrit les principes retenus par le CHU de Nantes pour la gestion des accès fournisseurs.

Le CHU de Nantes est certifié ISO27001 et Hébergeur de Données de Santé. Dans le cadre des intégrations, le respect de ce cadre sera exigé selon les processus en vigueur.

Cette annexe doit permettre aux candidats de répondre aux différentes consultations émises par le CHU de Nantes en proposant une solution technique adaptée et optimisée à l'environnement cible.

Les candidats devront se conformer aux infrastructures et standards techniques mis en place ainsi que les « bonnes pratiques » recommandées par l'ANSSI.

Le respect de cette annexe technique ne présuppose pas de l'implémentation qui devra être validée par les équipes des services numériques.

2. DOCUMENTS DE REFERENCE

PSSI CHU de Nantes

Annexes techniques CHU de Nantes

3. ACCES PHYSIQUES

Le fournisseur qui demande l'accès à des équipements doit à tout moment pouvoir justifier de son identité.

Dans le cas de demandes d'accès au Datacenter, un contrôle via le pc sécurité du site est imposé pour identification et sous réserve de validation des équipes de la Direction des Services Numériques concernées.

Tout accès au datacenter devra se faire en présence du CHU de Nantes.

4. ACCES DISTANT

L'accès à distance est un service fourni par le CHU de Nantes afin de permettre au fournisseur d'accéder aux ressources dont il a la charge, afin d'en assurer l'installation, la mise à jour et le maintien en condition opérationnel.

Conformément à nos principes d'infrastructure et de sécurisation des accès, dans le cadre de notre certification ISO 27001 et HDS, la connexion sur une machine de rebond est imposée.

La mise en œuvre de ce type d'accès est obligatoirement soumis à la validation du RSSI de l'établissement et peut-être suspendue à tout moment.

La cinématique est donc la suivante :

- Connexion au portail web
- Accès à une station de rebond avec un compte dédié
- Accès à la ressource à manager (serveur, pc, …) avec un autre compte dédié.

Une authentification complémentaire de type 2FA est déployée, accessible via le portail de connexion.

Aucun accès de type client VPN ne sera accepté.

4.1 Horaires de connexion

La plage de connexion autorisée et accessible sur demande correspond au créneau 8h-18h. En dehors de ces horaires, les connexions sont à proscrire, sauf dans le cadre de l'astreinte et assistance suivant contractualisation.

Les demandes de connexions « en mode projet », hors cadre de l'assistance en astreinte et sans supervision des référents techniques/fonctionnels nommés pour le suivi du projet, sont refusées.

4.2 Authentification et traçabilité

Toutes les traces de connexions sur le SI sont enregistrées et auditées via un SIEM.

4.2.1 OS Microsoft Windows

L'authentification du fournisseur s'appuie sur l'annuaire Active Directory du CHU.

Pour raison de sécurité, le compte est par défaut désactivé et réactivé à la demande du fournisseur.

Les mots de passe associés à chaque compte sont à modifier à minima une fois par an, de complexité forte.

4.2.2 OS de type Linux

Le fournisseur s'engage à fournir la clé publique SSH qui sera déployée sur les serveurs mis à disposition.

Les bonnes pratiques seront à appliquer, notamment l'élévation de droits via la commande "sudo". Le mot de passe du compte root ne sera pas transmis.

Les mots de passe associés à chaque compte sont à modifier à minima une fois par an, de complexité forte.

4.3 Transferts de fichiers

La solution proposée support le transfert de fichiers de petits volume uniquement ainsi que le copier/coller.

Si un chargement important (> 100Mo) est nécessaire, il faut alors anticiper le besoin via votre contact CHU afin de définir d'un point de dépôt des sources.

4.4 Enregistrement

Les actions réalisées dans le cadre de la connexion sont susceptibles d'être enregistrées et analysées si besoin.

4.5 Environnement de connexion

4.5.1 Client Citrix

La plateforme de connexion proposée s'appuie sur une infrastructure Citrix, via la mise à disposition de bureau publié.Pour un meilleur confort d'utilisation, il est possible d'installer le client Citrix Workspace sur le poste de prise de main du fournisseur si celui-ci l'autorise. Sinon le mode HTML5 est supporté nativement par le navigateur.

4.5.2 Gestion des données

Le système hébergeant la session temporaire est redémarré lors de la déconnexion de l'utilisateur. Toute données stockée sur cet espace sera automatiquement perdue.

4.5.3 Applications standards

Le CHU de Nantes met à disposition sur la machine de rebond des outils standards de production pour la connexion aux différentes ressources serveurs.

La liste ci-dessous n'étant pas exhaustive :

- Client SSH
- Client mRemote
- Client WinSCP
- Navigateur Web
- Client Oracle SQL Developper ou équivalent.
- Notepad++

L'installation sans autorisation d'applications non référencées est interdite. Celles-ci seront supprimées lors du redémarrage du serveur.

4.6 Installation sur les serveurs applicatifs

Conformément aux annexes techniques fournies par le CHUN, l'installation d'applications non utiles au bon fonctionnement de l'application est interdite.

Par exemple, l'installation de notepad++ sur le serveur application n'est pas autorisée et sera désinstallé.

Le principe de moindre privilège est appliqué ainsi que la réduction de la surface d'attaque.