



ANNEXE 3

CCTP DSI

FOURNISSEURS EXTERIEURS >>

Janvier 2025

INTRODUCTION

Face à la multiplication des cyberattaques ciblant aussi bien les entreprises privées que les institutions publiques, notamment les hôpitaux, la réglementation en matière de sécurité informatique évolue constamment. Cette évolution vise à adapter les normes et exigences de sécurité pour garantir une protection renforcée des équipements connectés, qu'ils soient reliés en Wi-Fi ou en filaire.

Le guide d'hygiène sécurité de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) énonce les mesures de sécurité à appliquer pour les équipements utilisés (<https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique>).

ARTICLE I – POSTES DE TRAVAIL

- 1. Système d'exploitation :** L'équipement sera au minimum sous système d'exploitation **Windows 11 Professionnel, version 24H2 ou ultérieure**. Le soumissionnaire devra respecter les recommandations de l'éditeur concernant la fin de support du système d'exploitation.

Le système d'exploitation **Windows 10** est encore accepté les versions LTSC 1809 (Long-Term Servicing Channel) ou supérieure supportée par Microsoft. Toute version inférieure ou sans support actif sera refusée.

Le Système d'exploitation Windows 7 est refusé car plus supporté depuis le 14/01/20 en termes de patch sécurité Microsoft.

Système d'exploitation (OS)	Version	Date de fin de support
Windows 11	Windows 11 Pro 24H2	13/10/2026
	Windows 11 Enterprise LTSC 2024	09/10/2029
	Windows 11 IoT Enterprise LTSC 2024	09/10/2029
Windows 10	Windows 10 Enterprise LTSC 1809	janv-29
	Windows 10 Enterprise LTSC 2021 (21H2)	12/01/2027

Tableau 1 - Fins de support sous Windows

Les équipements utilisant macOS doivent être au minimum sous macOS 14 (Sonoma) ou une version ultérieure. Les mises à jour de sécurité recommandées par Apple doivent être appliquées automatiquement. L'antivirus institutionnel Cortex de Palo Alto Networks devra être installé.

Système d'exploitation (OS)	Version	Date de fin de support
macOS	macOS 15 Sequoia	16/09/2027
	macOS 14 Sonoma	26/09/2026

Tableau 2 - Fins de support sous MacOS

Les **systèmes d'exploitation Linux** doivent être maintenus à jour automatiquement. L'antivirus institutionnel Cortex de Palo Alto Networks devra être installé.

Distribution	Version	Date de fin de support
Ubuntu	22.04 (Jammy)	04/2032
Debian	12 (Bookworm)	06/2033
Red Hat Enterprise Linux (RHEL)	9	05/2035

Tableau 3 - Fins de support sous Linux

- Mises à jour et gestion de l'obsolescence :** Les fournisseurs de matériel s'engagent à mettre à jour le matériel et à suivre les mises à jour et montées de version logiciels afin de garantir la sécurité du système d'information. Les mises à jour doivent être assurées par le fournisseur en collaboration avec le service. La DSI se réserve le droit d'appliquer automatiquement toutes mises à jour critiques de sécurité nécessaires au bon fonctionnement du Système d'Information.
- Application non fournie par la DSI :** La DSI ne fournira aucun logiciel payant sur du matériel ne lui appartenant pas. L'acquisition et la gestion de ces logiciels restent à la charge du fournisseur des équipements ou du service concerné.
- Anti-virus :** L'équipement devra être compatible avec l'anti-virus institutionnel Cortex de Palo Alto Networks. Il sera possible d'exclure des programmes exécutables mais cela ne serait fait qu'en cas de conflit ou de problèmes de performances.
- Accès au réseau institutionnel :** L'équipement devra être intégré dans le domaine Active Directory, il se verra donc appliquer nos politiques de sécurité qui excluent les comptes disposant de façon permanente des droits d'administration, en dehors de ceux utilisés par nos personnels autorisés.

En intégrant le domaine Active Directory institutionnel, l'équipement sera renommé selon la nomenclature en vigueur :

- Si équipement **BIOMED SUN**, alors **BIOSUNxxxxxxx**
- Si équipement **DRCI**, alors **DRISUNxxxxxxx**
- Si équipement **AUTRE**, alors **SUNNAPxxxxxxx**

En cas de problèmes de fonctionnement liés au besoin de l'application de disposer de privilèges, ceux-ci seront étudiés au cas par cas et toutes les modifications nécessaires seront apportées. Ce n'est qu'en cas d'impasse technique bloquante et sans escalade de support possible que le fonctionnement de l'application, sous un compte ayant les droits administrateurs permanents, sera envisagé.

Si l'intégration dans le domaine n'est pas réalisable, une étude sera menée avec la DSI.

- Télémaintenance :** La télémaintenance n'est possible que via la solution proposée par l'AP-HP (VPN, WALLIX-BASTION) pour un accès sécurisé sur le réseau institutionnel. L'utilisation de tout autre logiciel est interdite. Un compte VPN nominatif sera fourni, celui-ci sera sous la responsabilité d'une personne physique désignée chez le fournisseur. Il sera expressément demandé aux intervenants de veiller à fermer les sessions bureau à distance ouvertes sur le serveur en fin d'intervention et de ne PAS les laisser en tant que session déconnectée.

Si des données techniques sont remontées par la télémaintenance, cette fonctionnalité devra être conforme avec les règles du RGPD. Un DPO ou un DPD doit être désigné chez le fournisseur.

- 7. Stockage de données sur l'équipement :** Une solution de sauvegarde devra être établie par le soumissionnaire qui fournira une estimation de la volumétrie sur 12 mois en exposant la validité des données à longs termes.

Afin de se prémunir de toutes pannes matérielles, cette sauvegarde sera effectuée sur un partage réseau Windows et non sur des disques durs locaux à condition que le poste soit intégré au domaine Active Directory. Si le stockage réseau n'est pas possible, la station devra disposer d'un système de redondance au niveau des disques durs afin d'éviter la perte de données.

ARTICLE II – SERVEURS ET MACHINES VIRTUELLES

Ci-dessous la disponibilité et les dates de fin de service segmentées par systèmes d'exploitation et version :

- 1. Sous WINDOWS :** Le serveur sera au minimum sous système d'exploitation Windows 2022 64 bits versions FR ou US. Le soumissionnaire devra respecter les recommandations de l'éditeur concernant la fin de support du système d'exploitation.

Système d'exploitation (OS)	Version	Date de fin de support
Windows Server	Windows Server 2025	10/10/2034
	Windows Server 2022	14/10/2031
SQL Server	SQL Server 2022	11/01/2033
	SQL Server 2019	08/01/2030

Tableau 4 - Fins de support sous Windows Serveur

- 2. Sous LINUX :** Si l'équipement est installé avec un système d'exploitation Linux, les règles de sécurité devront être appliquées dans la mesure du possible :
- Il faut que les mises à jour Linux soient appliquées automatiquement.
 - Les fonctionnalités configurées au niveau des services démarrés doivent être configurés au strict minimum.
 - L'antivirus institutionnel Cortex de Palo Alto Networks sera installé.
- 3. Serveur physique :** Si le projet inclus la mise à disposition d'un serveur physique, celui-ci devra répondre à minima aux prérequis matériels suivants :
- Format rackable 1U ou 2U. Les formats TOUR même intégrables sont à proscrire.
 - 2 alimentations redondantes
 - 2 Ports Ethernet

4. **Serveur virtuel** : Si le projet inclus la mise à disposition d'une machine virtuelle, celle-ci devra se présenter de préférence dans le format OVA et respecter la norme de compatibilité VMWARE 7.0.

En cas de mise à disposition d'une machine virtuelle, l'unité par défaut est la suivante :

- Serveur virtualisé VMware 7
- OS Windows 2022 FR ou US
- 2 VCPU.
- 8 Go de RAM,
- 1 disque (70Go disque système +application), préciser si besoins/demandes spécifiques.

- 5. Mises à jour et gestion de l'obsolescence :** Le serveur se verra appliquer automatiquement toutes les mises à jour critiques de sécurité disponibles via Windows Update suivant un calendrier défini en fonction des fenêtres possibles de redémarrage. Toute dérogation à cette règle et mise en place d'un circuit de validation des mises à jour devra être définie en concertation fournisseur/ Direction du Système d'Information avant le passage en production.
- 6. Anti-virus :** Le serveur sera compatible avec l'anti-virus institutionnel Cortex de Palo Alto Networks. Il sera possible d'exclure de son champ des programmes exécutables, néanmoins cela ne sera fait qu'en cas de conflits ou de problèmes de performances.
- 7. Domaine Active Directory :** Le serveur sera être intégré dans le domaine Active Directory, il se verra donc appliquer nos politiques de sécurité qui excluent les comptes disposant de façon permanente des droits d'administration, en dehors de ceux utilisés par nos personnels autorisés..

En intégrant le domaine Active Directory institutionnel, l'équipement sera renommé selon la nomenclature en vigueur (*Trigramme du site -XXX (15 caractères Max) ou SUNxxxx*) :

Hôpital	Trigramme
Pitié-Salpêtrière	PSL
Charles-Foix	CFX
Saint-Antoine	SAT
Tenon	TNN
Rothschild	RTH
Armand-Trousseau	TRS
La Roche-Guyon	TRS

En cas de problèmes de fonctionnement liés au besoin de l'application de disposer de privilèges, ceux-ci seront étudiés au cas par cas et toutes les modifications nécessaires seront apportées. Ce n'est qu'en cas d'impasse technique bloquante et sans escalade de support possible que le fonctionnement de l'application, sous un compte ayant les droits administrateurs permanents, sera envisagé.

- 8. L'accès internet :** Il sera nécessaire d'indiquer ce besoin avant le déploiement du serveur sous réserve de la validation du RSSI et la présence d'une matrice de flux.

9. Conditions lancement process/service :

Aucun process/service ne doit être lancé :

- Sous un compte personnel (code APH personnel APHP ou code 7xxxxxx attribué aux intervenants des fournisseurs/extérieurs).
- Sous un compte local de la machine.

Si une application inclut des process applicatifs, ceux-ci devront dans la mesure du possible être lancés en tant que SERVICE Windows. Le fonctionnement en tant qu'application Windows ordinaire dans une session (depuis un bureau) est fortement déconseillé.

Un compte Active Directory générique ou de service sera fourni le cas échéant. Les comptes personnels (_7xxxxx) fournis aux intervenants doivent être réservés aux opérations d'installations ou de télémaintenances pour des connexions interactives.

Si ce mode est incontournable :

- La session sera ouverte sous un compte générique Active Directory,
- Elle sera ouverte sur la console du serveur et non dans une session bureau à distance. Si l'application est démarrée automatiquement, le fournisseur devra placer les raccourcis dans le dossier Démarrage du compte concerné UNIQUEMENT et NON dans celui commun à tous les comptes ("All users" ou équivalent).

10. Application utilisant des données pérennes sur le serveur (fichiers à plats ou bases de données) :

Une politique de sauvegarde devra être définie et mise en œuvre en concertation avec le service informatique avant le passage en production. Une période de rétention devra être définie.

La mise en place de cette sauvegarde devra prendre en compte la notion de PDMA (Perte de Données Maximales Admissibles) ou perte de données maximales acceptables pour le métier (exprimée en temps).

Les données sauvegardées seront à déposer sur un partage (NFS/CIFS) mis à disposition par nos équipes (partages accessibles via le compte de service active directory générant les sauvegardes). Les données sauvegardées ne devront en aucun cas être conservées/stockées sur les disques locaux du serveur.

Dans le cas d'une machine virtuelle, la sauvegarde système sera faite de manière intégrale au minimum une fois par jour. Dans le cas d'un serveur physique, la sauvegarde système devra être évoquée en tenant COMPTE de la DIMA (Durée d'Interruption Maximale Admissible).

11. Documentation :

Un document d'exploitation informatique du serveur devra être fourni, spécifiant notamment les programmes, fichiers de log, espace disque à surveiller, et éventuellement les sauvegardes à faire. Des redémarrages de serveur seront peut-être nécessaires suite à des mises à jour de sécurité de Microsoft. Ce document devra nous signaler les plages horaires et des modalités de ces redémarrages planifiés.

12. Fermeture automatique des sessions :

Sur de nombreux serveurs, une politique de fermeture automatique de session en cas d'inactivité (1H) et de session déconnectée (5Min) est déployée. En cas de besoin d'exclusion (patch ou script session ouverte avec temps d'exécution long) merci de nous demander une exception à cette règle en nous indiquant le serveur devant bénéficier de cette exclusion.

13. Télémaintenance : La télémaintenance n'est possible que via la solution proposée par l'AP-HP (VPN, WALLIX-BASTION) pour un accès sécurisé sur le réseau institutionnel. L'utilisation de tout autre logiciel est interdite. Un compte VPN nominatif sera fourni, celui-ci sera sous la responsabilité d'une personne physique désignée chez le fournisseur. Il sera expressément demandé aux intervenants de veiller à fermer les sessions bureau à distance ouvertes sur le serveur en fin d'intervention et de ne PAS les laisser en tant que session déconnectée.

Si des données techniques sont remontées par la télémaintenance, cette fonctionnalité devra être conforme avec les règles du RGPD. Un DPO ou un DPD doit être désigné chez le fournisseur.

14. Supervision standard embarquée :

Une surveillance CPU/RAM/CCU/Espace Disques/Services en "démarrage automatique".

En cas de demandes supplémentaires de supervision, il faudra nous faire parvenir les besoins pour une étude de mise en œuvre.

ARTICLE III – TABLETTES CONNECTEES

Les systèmes Windows seront gérés à l'identique les postes de travail (voir Article 1).

Les appareils Android doivent être à jour et seront obligatoirement soumis aux solutions Workspace ONE (MDM) ou INTUNE afin de créer des cas d'usage et de verrouiller les tablettes selon les normes de la DSI.

Pour tout autre système d'exploitation, une étude et une validation par la DSI sera nécessaire.

ARTICLE IV – CAMERA SUR IP

Suite aux différentes cyber-attaques sur des entreprises privées et des institutions publiques (notamment des hôpitaux), les normes de sécurité informatique pour du matériel informatique qui se connecte à un réseau informatique (en wifi ou en filaire) deviennent plus restrictives.

1. Les mots de passe par défaut doivent être remplacés par des mots de passe robustes et spécifiques au service dans lequel ils sont déployés. Il ne faut pas qu'ils soient les mêmes que chez d'autres clients.
2. Les dernières mises à jour de microcode (Firmware) doivent être appliquées pour des mesures de sécurité.
3. La caméra devra être connectée au réseau informatique en filaire. Le protocole wifi devra être activé seulement au moment des mises à jour de microcode.
4. Si la caméra enregistre des données médicales et donc des données patient, le fournisseur s'engage dans ce cadre-là sur les clauses contractuelles de sous-traitance en conformité au RGPD. Un DPO ou un DPD doit être désigné chez le fournisseur.