

## Durcissement de l'OS (Système d'Exploitation)

- Limiter les applications installées et modules optionnels des navigateurs web aux seuls nécessaires ;
- Limiter les rôles et services au juste besoin sur les serveurs dotés d'un OS Microsoft ;
- Doter les postes utilisateurs d'un pare-feu local et d'un anti-virus ;
- Les agents antivirus doivent être déployés sur l'ensemble des postes informatiques (Serveur et postes de travail) à l'exception du serveur vidéo et des 2 serveurs enregistreurs ;
- Désactiver les exécutions automatiques (autorun) ;
- Désactiver Windows auto-update ;
- Mise en place de mot de passe d'accès au BIOS ;
- La séquence de démarrage des postes clients et serveur ne doit autoriser que la partition d'amorçage du disque dur ;
- Sauvegarde régulière et stockée sur un équipement déconnecté et dédié au système ;
- Arrêt automatique des serveurs lors de la perte de courant et lorsque la limite de l'onduleur arrive à la moitié de sa capacité ;
- Login nominatif ;
- Les droits utilisateurs doivent être limités au strict nécessaire ;
- Les privilèges d'administration ne doivent pas être utilisés pour les différents applicatifs constituant le CADIVS ;
- Mot de passe avec renouvellement automatique (périodicité à définir avec le client final) ;
  - Complexité :
    - 9 caractères minimum ;
    - 14 pour les comptes d'administration ;
    - Utilisation de 3 types de caractères différents sur les 4 possibles (Majuscule, minuscule, chiffre et caractères spéciaux) ;
- Mise en place d'une politique USB (white liste) ;
- Synchronisation de l'heure de tous les éléments constituant le S2I.

Cf :

Guide d'hygiène informatique de l'ANSSI.

<https://www.ssi.gouv.fr/administration/guide/guide-dhygiene-informatique/>

Exigences de sécurité matérielles

[https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-exigences\\_securite\\_materielle.pdf](https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-exigences_securite_materielle.pdf)

Recommandations relatives à l'administration sécurisée des systèmes d'information

<https://www.ssi.gouv.fr/administration/guide/securiser-ladministration-des-systemes-dinformation/>