# Installation des postes de travail au sein de Logeas informatique (procédure #58)

| | |
|---|---|
| **Suivi des modifications majeures** | 20/05/2019 - Nicolas MARCHAND - Création |
| **Suivi des approbations** | Elément ProjeQtor Document # 58 |
| **Objet** | Préconisation sur les postes collborateur dans la sscop |
| **Destinataires** | **- Validation des modifications :** Gérant<br>**- Approbation du document** : Tous |

## Ordinateur fixe & portable "Physique"

### Session Windows

Du côté du Cloud, il est fortement recommandé de renoncer à l'authentification sur le poste par le biais d'un compte Microsoft. Dans le cas contraire, des paramètres sensibles, comme les clés de chiffrement BitLocker, sont stockés sur les serveurs de l'éditeur. Ce type d'ouverture de session devrait donc être bloqué, tout comme le stockage Cloud OneDrive.
Ce service est particulièrement bien intégré à Windows 10. “L’utilisation aisée du service représente une tentation forte pour les utilisateurs d’y stocker des données professionnelles” note l'ANSSI. Pour des questions de confidentialité des données, elle juge donc “préférable de désactiver l’accès au service.”
(http://www.zdnet.fr/actualites/les-bons-tuyaux-de-l-agence-de-securite-francaise-pour-utiliser-windows-10-39847868.htm)

### Crytage du disque

**TOUT disque** qui contiens soit :

- des informations liés à l'entreprise (en particulier la réplication du cloud)
- des bases de données de LoGeAs
- des sauvegardes de l'entreprise ou des clients

**DOIT ETRE CRYPTER, par sécurité on crytera aussi les disques systéme de ces postes.**

La solution retenu est l'utilisation de **BitLocker**

On prendra en compte les points suivant :

- le mot de passe doit être long, on recommande l'usage d'un vers de poème
  On utilisera le même mot de passe pour tout les disques
  Remarque : ce mot de passe n'est saisie qu'une fois au démarrage de la machine. Attention lors du lancement du poste il est a saisir sur un clavier qwerty.
- l'écran de veille doit être activé et doit necessiter la saisee du mot de passe au dévérouillage.
  On mettre un temps de veille court (inférieur à 10 minutes)
  Remarque : afin déviter les resaisies du code windows, les postes seront pourvus de lecteur d'empreinte.

- les “Clés de récupération du chiffrement de lecteur BitLocker” doivent être stocké dans une note sécurisé de dashlane avec le titre “Ordinateur de XXX”. Elle sera partagé avec le gérant. Elle ne sont pas stocké ailleurs.

### Ressource

- http://www.octetmalin.net/windows/tutoriels/bitlocker-crypter-disque-systeme-sans-peripherique-puce-tpm.php