d’empreinte digitale est également justifiable, car, si à l’avenir, son utilité est souhaitée, aucun besoin de racheter du matériel.

Nous laissons désormais libre choix à notre DSI pour le choix de la machine qui lui convient.

Ecologie

Norme :

- ISO 9001
- ISO 14001
- ISO 27001
- ISO 45001
- ISO 50001

Certification :

- 80 Plus
- Éco-déclarations (respecte la norme ECMA 370(en anglais))
- ENERGY STAR
- EPEAT
- Conformité règlementaire Recyclage
- TCO

Logiciel et cybersécurité

Choix des logiciels et explications :

Notre choix de système d’exploitation s’est porté sur Windows 11 Pro. Nous laisserons le soin au service comptabilité de faire l’achat de licences que nous pourrons activer sur chaque machine, grâce au service de déploiement automatique adéquat pour installer l’OS sur les postes.

Ce choix est motivé par le besoin de fournir à nos employés une interface et un système simple d’usage et familier. W11 permet de s’assurer que les machines profiteront des dernières mises à jour de sécurité, ainsi qu’une compatibilité totale des logiciels de bureautique tel que Microsoft Office, sur lesquels la majeure partie des utilisateurs sont déjà familiarisés. Apple aurait été beaucoup trop cher et très peu écologique, et l’environnement Linux aurait pu être un choix très intéressant, mais nous pensons que le temps à investir dans la formation des utilisateurs n’est pas rentable.

Nous ferons en sorte d'automatiser la désinstallation de logiciels préinstallés, bloquer l'installation de futurs logiciels inutiles que Microsoft pousse de temps en temps et limiter autant que possible la télémétrie de l'éditeur.

Le déploiement d'un antivirus réputé, comme SentinelOne ou CarbonBlack est obligatoire, également bien paramétrer les navigateurs internet afin de bloquer les cookies tiers, forcer l'usage d'adresses HTTPS etc. Également, un système de prise de contrôle à distance, comme TeamViewer, afin d'avoir un accès pour venir en aide aux utilisateurs.

Chaque machine aura deux sessions, une « administrateur », avec nos accès privés. Une session « utilisateur » qui sera celle de l'utilisateur, afin de limiter les accès et les éventuelles erreurs.

Nous n'avons pas d'information concernant un éventuel serveur. Si jamais il existe, il sera parfaitement adapté. Car les utilisateurs pourraient se connecter à une session à distance, par le biais d'une connexion VPN et ils pourraient donc travailler sans jamais stocker une quelconque information sensible. Dans le doute, nous allons donc nous assurer de chiffrer les données du stockage interne par le biais de Bitlocker, nous stockerons les clés de chiffrement dans notre Active Directory.

En parlant d'AD, il serait judicieux de mettre toutes les machines en domaine, ainsi, elles auraient automatiquement des GPO et des accès spécifiques à des serveurs ainsi qu'a des imprimantes, partout en déplacement.

Bien entendu, la création de mot de passe pour accéder à leur session se fera en accord avec les dernières recommandations de la CNIL, transmission uniquement orale ou par SMS à l'utilisateur. Et la création d'un système de double authentification, via une application par authentificateur, comme Microsoft Authenticator, Google Authenticator ou encore Duo Mobile.