

**Pour définir efficacement ces accès physiques, il convient :**

1. D'identifier les zones à protéger (notamment les accès aux serveurs et les postes de travail contenant les informations sensibles).
2. De mettre en place des outils de contrôle d'accès, suivant le niveau de sécurité exigé (badge, sas, personnel d'accueil, procédés biométriques, etc.), et de surveillance (caméras, détecteurs, etc.).
3. De verrouiller les postes de travail par un mot de passe **complexe**.
4. De verrouiller la session en quittant le poste de travail.
5. D'empêcher l'utilisation des ports USB et lecteurs CD/DVD, pour éviter la copie de fichiers et le démarrage de l'ordinateur par ces biais.
6. De fermer les bureaux à clé.
7. De conserver les doubles des clés (physiques et de chiffrement) dans des lieux sûrs.
8. D'établir des règles pour les visiteurs (interdiction d'introduire des clés USB, des téléphones portables ou baladeurs MP3, des ordinateurs portables, accompagnement constant des visiteurs dans l'entreprise, vérification et enregistrement des identités).
9. De prendre en compte la dimension sécurité dans le choix des prestataires de services type nettoyage et gardiennage (demande des CV, références, définir des clauses de confidentialité).
10. De responsabiliser et éduquer le personnel.

**e ■ VERROUILLER IMPÉRATIVEMENT SON ORDINATEUR EN QUITTANT SON BUREAU**

Une règle d'or en la matière !

Si un intrus parvient à s'introduire dans les locaux de l'entreprise, il tentera inévitablement de se connecter au premier ordinateur venu pour atteindre le réseau et l'ensemble des documents partagés. Il peut aussi cibler directement l'ordinateur d'un service précis, pour consulter la messagerie, accéder aux outils de *workgroup* installés (il trouvera inévitablement un lien direct présent sur le bureau de l'ordinateur pour accéder à ces outils) ou bien encore installer un cheval de Troie.

Certes, même si l'ordinateur est verrouillé, un intrus expérimenté arrivera peut-être à contourner les mesures de sécurité – avec difficulté, cependant –, mais lui compliquer la tâche en verrouillant son ordinateur au moment de quitter son poste n'est pas superflu ! C'est un peu comme si un commerçant laissait les clés de sa caisse sur le comptoir avant de s'absenter...