## 7. INTERNET

*Un formidable outil de productivité mais qui peut apporter son lot de problèmes.*

**Internet est-il forcément votre ami ?**
Internet est peuplé d'inconnus qui sont tous vos «amis» !
Internet n'est pas sans foi ni loi.
Le droit du monde réel s'applique à l'Internet.
Evitez d'aller sur des sites à risques (utilisez un outil comme WOT pour vous prévenir).
Attention aux propositions alléchantes, la gratuité n'existe jamais, même sur Internet !
La plupart des fichiers sur les sites de téléchargements illégaux intègrent des programmes malveillants.
Evitez d'avoir un comportement à risque.

## 8. APPLICATIONS

*Qui n'a jamais téléchargé une application, un utilitaire ou un Plug-in ?*

**Êtes-vous sûr d'avoir besoin de toutes vos applications ?**
Evitez d'installer n'importe quoi sur votre ordinateur.
Les logiciels gratuits ou piratés intègrent souvent des logiciels malicieux ou des failles de sécurité.
Faites le ménage régulièrement dans vos applications.
Installez des applications dont vous avez vraiment besoin.
N'installez pas de logiciels qui ne sont pas adaptés aux performances de votre ordinateur (e.g. outils de CAO).
Vérifiez qu'il reste suffisamment d'espace libre sur le disque dur de votre ordinateur (5 à 10%).

## 9. PRESTATAIRES

*Travailler ensemble, c'est une confiance à mettre en place et des règles à suivre.*

**Avez-vous pris toutes les précautions vis-à-vis de vos partenaires ?**
Accord de confidentialité.
Charte informatique.
Attention aux données à caractère personnel auxquelles ils pourraient avoir accès.
Attention à l'accès Internet.
Ne laissez pas des prestataires seuls dans vos locaux notamment les locaux informatiques.
Attention aux accès distants pour la maintenance (serveurs, centraux téléphoniques, photocopieurs…).
Attention aux prestataires travaillant pendant les heures et jours non-ouvrés.

## 10. ACCES PHYSIQUES

*Sans aller jusqu'aux portes blindées, aux badges à triple serrures électroniques, ne laissez pas certains secteurs de l'entreprise en libre accès.*

**Pensez-vous à fermer les portes et les fenêtres ?**
Les 9 commandements précédents sont inutiles si votre entreprise est en « accès libre ».
L'accès physique à votre entreprise doit être contrôlé.
Les locaux informatiques et techniques doivent faire l'objet d'une attention particulière (accès par clé et/ou par badge, traçabilité, nombre réduit de personnes habilitées).
Privilégiez les bureaux sans-papier le soir, le week-end et pendant les vacances.
Utilisez des broyeurs de papier pour les documents confidentiels.

NOS PARTENAIRES



Gendarmerie nationale

# LES 10 COMMANDEMENTS DU CHEF D'ENTREPRISE


## SECURITE DES SYSTEMES D'INFORMATION

Même si la sécurité à 100 % n'existe pas, certaines recommandations de base sont utiles pour se protéger des risques les plus courants. Les PME-PMI sont particulièrement vulnérables vis-à-vis des attaques informatiques visant à récupérer des données sensibles ou à paralyser leur système d'information.

## 1. L'INVENTAIRE DU PATRIMOINE

*Première étape : bien identifier les données vitales de l'entreprise.*

**Quelles sont les données vitales pour votre entreprise ?**
Documents (bureautiques, financiers, marketing…).
Listes de clients, fournisseurs…
Images, vidéos.
Brevets.
Mails.
Favoris de votre navigateur.
Etc.

## 2. LES SAUVEGARDES

*C'est évident, mais encore faut-il les rendre systématiques, ciblées et fiables.*

**Avez-vous pensé à sauvegarder vos données** ?
Triez, classez et donnez des noms pertinents à vos documents.
Recherchez l'exhaustivité maximale de vos données à sauvegarder.
Utilisez un logiciel de sauvegarde dédié.
Faites au moins une sauvegarde par jour.
Externalisez vos sauvegardes hors de l'entreprise.
Testez vos sauvegardes régulièrement.
Pensez aux outils de synchronisation si vous avez plusieurs ordinateurs.

**Tenez vous informé** :

www.securite-informatique.gouv.fr/

## 3. MOT DE PASSE

*Indispensable, incontournable et pourtant se résumant le plus souvent au prénom de votre enfant griffonné sur un bout de papier dans un tiroir du bureau !*

**Êtes-vous sûr d'avoir un mot de passe robuste ?**
Utilisez au moins 8 caractères.
Utilisez au moins 1 chiffre et 1 caractère accentué.
Facile à retenir mais difficile à deviner (trouver un moyen mnémotechnique).
N'utilisez pas un mot de passe qui contient des informations personnelles (date de naissance, de mariage…).
Renouvelez régulièrement (tous 3 mois).
Utilisez différents mots de passe suivant les accès (compte bancaire, messagerie...).
Ne stockez pas les mots de passe dans un fichier ou sur un support papier.

## 4. SECURISER LE POSTE DE TRAVAIL

*Un seul poste de travail non sécurisé et le réseau tout entier peut tomber.*

**Votre poste de travail est-il sûr ?**
Utilisez-vous un antivirus ? Se met-il à jour automatiquement ? (au moins 1 fois/jour voire 1 fois/heure).
Votre système d'exploitation est-il à jour ? Se met-il à jour automatiquement ?
Votre navigateur internet est-il à jour ? Se met-il à jour automatiquement ?
Les plug-ins de celui-ci sont-ils à jour ?
Avez-vous un pare-feu personnel ?
Attention aux périphériques USB, vecteurs de codes malveillants (clés, disques durs…).

## 5. SENSIBILISATION

*Vous êtes conscient de l'importance de la sécurité et motivé à la mettre en place. Et vos collaborateurs ?*

**Votre personnel a-t-il conscience des risques ?**
Soyez conscient que les utilisateurs sont le maillon faible.
Pensez à leur donner les règles de base.
Pensez à leur faire signer une charte informatique (charte d'utilisation des moyens informatiques).
Ne confondez pas usage privé et usage professionnel des outils informatiques (ordinateurs portables, smartphones...).
Attention à la divulgation de données professionnelles (médias sociaux…).
Communiquez régulièrement sur les risques et les nouveaux dangers.

## 6. MAILS, CANULARS ET PIECES JOINTES

*75% des attaques et infiltrations passent par le mail.*

**Etes-vous vigilant ?**
N'ouvrez pas, ne répondez pas, mais supprimez directement les mails provenant d'expéditeurs inconnus.
Ne cliquez pas sur les liens inclus dans les mails si vous avez le moindre doute.
Ne cliquez pas sur les pièces jointes incluses dans les mails si vous avez le moindre doute.
Ne relayez pas les messages de type chaînes de lettres, porte-bonheur…
Jamais votre banque ne vous demandera un mot de passe (ou sa réinitialisation par un lien) ou un code pin par mail (social phishing !).
Attention aux liens malveillants sur les médias sociaux.