

# Une meilleure sécurité de l'information pour les PME

Le programme en 10 points pour une protection IT basique efficace



La présente brochure se base sur les «Dix règles d'or de la sécurité de l'information dans les PME» du groupe spécialisé PME de la fondation InfoSurance. [www.infosurance.ch/de/kmu.htm](http://www.infosurance.ch/de/kmu.htm)

**Conception et texte:**

Dr Calista Fischer, Fondation InfoSurance

**Impression et composition:** Fotorotar AG, Egg bei Zürich

**Tirage:** 60 000

**Copyright:**

Fondation InfoSurance, Badenerstrasse 551, 8048 Zurich, Tel. +41 43 311 19 19, [www.infosurance.ch](http://www.infosurance.ch)  
La diffusion gratuite du contenu de cette brochure est autorisée avec indication de la source et correspond à l'esprit de la fondation.

La fondation InfoSurance n'assume aucune responsabilité pour les dommages éventuels qui pourraient résulter de l'application correcte ou incorrecte du programme en 10 points.

## Chères dirigeantes de PME, chers dirigeants de PME

Votre réputation est-elle en jeu, perdez-vous des clients ou devez-vous même payer des pénalités conventionnelles si vous ne pouvez pas livrer à temps une commande? En faisant référence à ces problèmes, savez-vous si votre entreprise pourrait continuer à produire ses prestations fondamentales, si votre réseau informatique s'arrêtait brusquement de fonctionner? Que votre entreprise utilise une centaine d'ordinateurs, ou qu'elle n'en utilise que trois, vous devez, en tant que membre de la direction, étudier périodiquement des questions de ce type.

Même une entreprise qui n'utilise son seul ordinateur que pour établir des factures et envoyer un e-mail de temps en temps, est soumise à l'obligation légale de conservation des données de l'entreprise, et au respect de la protection des données. Il suffit souvent de la contamination par un virus ou d'un défaut d'entretien d'un firewall pour contrevenir involontairement à ces obligations légales. Pire encore, des programmes malicieux peuvent conduire à la perte irrémédiable de données importantes, et même mettre en danger l'existence économique de votre entreprise.

Les pertes de données et les systèmes informatiques qui tombent en panne au cours d'une phase de production critique, suite à des attaques en provenance d'Internet, peuvent coûter très cher à la direction responsable! Particulièrement parce que le nombre d'attaques dirigées vers les réseaux d'entreprises a énormément augmenté au cours des dernières années, et que les mesures de protection sont devenues aujourd'hui une nécessité absolue. Celui qui ne se préoccupe pas de la mise en œuvre de mesures de protection suffisantes dans son entreprise, vit dangereusement. Un regard vers l'avenir le confirme: le thème de la sécurité de l'information est de plus en plus important pour toutes les entreprises. Dès aujourd'hui, les prestataires d'assurances professionnelles exigent de leurs clients un comportement toujours plus proactif en matière de sécurité, allant jusqu'à leur demander la preuve des mesures de protection visant à assurer la sécurité de leurs informations. Il est donc utile d'inclure régulièrement le thème de la sécurité de l'information dans les réunions de direction, et d'en discuter.

Vous apprendrez dans les pages suivantes comment améliorer la sécurité et la situation de votre entreprise, la disponibilité de vos données et de vos informations, et comment vous protéger contre les attaques malicieuses, qu'elles proviennent de l'intérieur ou de l'extérieur. L'objectif de notre programme en 10 points consiste à vous aider à introduire une protection de base efficace, de manière à éviter à l'avenir la perte de données vitales et à réduire au minimum les dommages financiers résultant d'une panne du système. Une check-list et une collection de liens vous aideront en outre à mettre en œuvre ce programme et vous permettront de contrôler les mesures de sécurité que vous aurez mises en œuvre.

Je vous souhaite, ainsi qu'à votre entreprise, beaucoup de succès et une sécurité de l'information améliorée.



Dr André Schmid  
Directeur de InfoSurance

«La sécurité s'appuie à parts égales sur des facteurs techniques, organisationnels et humains», tel est l'avis des plus grands experts en sécurité lorsqu'on leur demande comment améliorer la sécurité des systèmes d'information et de communication dans les entreprises. Les meilleures solutions de sécurité et les collaborateurs les plus motivés ne peuvent aboutir à une protection de base efficace que si la direction contribue également à l'amélioration de la sécurité.

- Désignez dans votre entreprise, même si vous n'employez que deux personnes, un responsable informatique et un responsable des technologies de l'information (IT), ainsi qu'un suppléant. S'ils ne possèdent pas les connaissances nécessaires pour remplir ces tâches, envoyez votre collaboratrice ou votre collaborateur suivre un cours approprié, ou travaillez avec un expert externe en sécurité IT. Un cours de trois jours ou un spécialiste externe coûtera sensiblement moins cher à votre entreprise que les conséquences d'une perte de données ou d'une infraction à la loi sur la protection des données.
- Toutes les tâches de sécurité déléguées au responsable IT interne ou à une personne externe, par exemple la génération des sauvegardes, doivent être définies par écrit et consigné dans un «Cahier des charges» (vous trouverez plus loin une liste des principales tâches du responsable IT).
- Contrôlez régulièrement si le responsable IT exécute correctement les tâches qui lui sont confiées.
- Toutes les collaboratrices et tous les collaborateurs qui travaillent sur un ordinateur doivent recevoir un règlement d'utilisation qui décrit les actions qu'ils peuvent exécuter sur leur ordinateur, et celles qui leur sont interdites (vous trouverez une proposition de règlement à la page 9, étape 8).

#### *Cahier des charges*

#### **Les tâches d'un responsable IT interne ou externe sont entre autres les suivantes:**

- Sauvegarder régulièrement les données des serveurs, clients (stations de travail), portables et autres appareils mobiles (voir étape 2).
- Mettre à jour les programmes antivirus, les firewall, systèmes d'exploitation et autres logiciels (voir étapes 3, 4 et 5).
- Etablir une liste de tous les ordinateurs existants dans l'entreprise, des programmes qui y sont installés ainsi que des mises à jour logicielles réalisées (voir étape 5).
- Administrer les droits d'accès – quel collaborateur peut exécuter quels programmes? À quelles données, informations, fichiers, etc. a-t-il accès?
- Etablir et mettre à jour une liste de toutes les personnes qui peuvent accéder à distance (Remote Access) au réseau d'entreprise, déterminer la durée des autorisations et les retirer après expiration. S'assurer que leurs programmes de protection sont à jour.
- S'assurer qu'aucune infraction à la loi sur la protection des données n'est engendrée du côté IT, en particulier en mettant à jour les divers programmes de protection (firewall, programmes antivirus) et en utilisant des mots de passe robustes (voir étapes 3, 4 et 7).
- Contrôler que les collaboratrices et les collaborateurs respectent les prescriptions IT (voir étape 8).
- Etre l'interlocuteur pour les questions de sécurité, le point de signalisation des événements concernant la sécurité – par exemple en cas de perte d'ordinateurs portables, de détection de virus, etc.

Les hackers et les virus ne sont pas les seules menaces qui guettent les données de votre entreprise. Des dangers comme l'incendie, les inondations, les courts-circuits peuvent conduire en cas de sinistre à une perte totale d'informations importantes. Cette situation est doublement désagréable, car le législateur impose également que les données d'entreprises soient conservées et archivées. Il faut impérativement éviter la perte des données de l'entreprise. C'est pourquoi les données doivent être régulièrement sauvegardées et archivées en toute sécurité, et les sauvegardes testées périodiquement.

- Les données électroniques doivent être enregistrées sur un support mobile comme une bande magnétique, un CD, un DVD ou une disquette. La fréquence de sauvegarde dépend de l'activité de la taille de votre entreprise. La sauvegarde complète de toutes les données doit au moins être réalisée une fois par semaine, et même tous les jours dans les entreprises de plus grande taille.
  - Définissez par écrit qui doit réaliser la sauvegarde des données, et à quelle périodicité il doit le faire. Établissez une liste de contrôle dans laquelle seront inscrites les sauvegardes exécutées (voir le cahier des charges du responsable IT, étape 1).
  - Toutes les données traitées dans l'entreprise doivent être sauvegardées – tous les fichiers, courriers, tableaux et e-mails dont le contenu a trait à l'entreprise.
  - De manière idéale, il faudrait également faire une sauvegarde de la configuration logicielle. En cas de panne totale du système informatique, vous pourrez économiser beaucoup de temps, car les logiciels seront plus rapides à réinstaller.
- **Important:** Les sauvegardes hebdomadaires, mensuelles et annuelles ne doivent pas être conservées dans l'entreprise, car elles seraient également détruites en cas d'incendie ou d'inondation! Les données qui n'existent que sous forme papier, par exemple les contrats et les certificats importants, doivent impérativement être copiés et stockés hors de l'entreprise. Lieux recommandés pour la conservation des copies de sauvegardes et des documents importants de l'entreprise : coffre bancaire ou à domicile.
  - Vérifiez régulièrement si les copies de sauvegardes sont encore lisibles!

### Exemple pour une entreprise avec sauvegarde quotidienne

- Sauvegardes quotidiennes: un support de données (CD, DVD ou disquette) pour le lundi, le mardi, le mercredi et le jeudi. Les copies quotidiennes sont écrasées le jour correspondant de la semaine suivante. Les sauvegardes quotidiennes sont conservées dans l'entreprise, mais hors du local du serveur.
- Sauvegardes hebdomadaires: chaque vendredi. Un support de données séparé doit être utilisé pour chaque vendredi du mois – à conserver hors de l'entreprise!
- Sauvegardes mensuelles: à la fin de chaque mois. Les sauvegardes mensuelles ne sont pas écrasées – à conserver hors de l'entreprise!

Internet et le courrier électronique sont des moyens de communication et d'informations indispensables pour le quotidien d'une entreprise moderne. Des programmes malicieux comme des virus peuvent paralyser ces infrastructures de communication et mettre en danger l'existence économique de l'entreprise. Outre les dommages directs, les systèmes informatiques insuffisamment protégés participent fréquemment à la diffusion des virus et sont exploités pour mener des attaques ciblées contre une entreprise tierce. Lorsqu'un dirigeant prend des mesures de protection insuffisantes pour son système informatique, il agit avec négligence et peut éventuellement être poursuivi pénalement.

- Les virus informatiques peuvent modifier, manipuler ou même détruire complètement les données et les programmes. Des programmes informatiques malicieux sont transmis par des fichiers joints à des e-mails (Attachments) ou par des supports de données comme des disquettes, etc. Sur Internet, les virus sont souvent cachés derrière des programmes gratuits utiles ou divertissants, activés d'un simple clic.
- La seule protection contre les virus connus est offerte par un programme antivirus qui identifie et neutralise les intrus dangereux comme les virus et les vers. Les programmes correspondants peuvent être achetés dans les magasins d'informatique ou être téléchargés gratuitement à partir d'Internet.
- Les hackers programment constamment de nouveaux virus. Les programmes antivirus doivent donc être constamment mis à jour. Selon le produit que vous utilisez, le programme recherche automatiquement les mises à jour les plus récentes sur la page d'accueil du fabricant. Informez-vous auprès de votre vendeur si votre programme est doté de cette fonctionnalité. Si ce n'est pas le cas, procédez à la mise à jour chaque semaine, ou même chaque jour.
- Pour que votre réseau soit protégé efficacement contre les virus et autres programmes dangereux, l'antivirus doit être installé et mis à jour régulièrement sur tous les serveurs et les postes de travail (Clients).
- Exécutez au moins une fois par semaine un «Virus-Scan » pour détecter et éliminer les virus qui auraient pu s'introduire sans être reconnus. Si vous échangez beaucoup de données, et en cas de suspicion de contamination par un virus, il est recommandé de procéder tous les jours à un Virus-Scan.
- Dans le cas des grands réseaux, la meilleure solution consiste à gérer automatiquement et de manière centralisée le programme antivirus et les mises à jour.
- La mise à jour des programmes antivirus doit être réalisée et contrôlée de manière particulièrement attentive sur les ordinateurs portables. En effet, ces appareils sont utilisés à l'extérieur et peuvent ainsi manquer une mise à jour importante, lorsqu'ils sont à nouveau raccordés au réseau d'entreprise.

**Conseils pour les prescriptions IT destinées aux collaboratrices et aux collaborateurs (voir également l'étape 8):**

- Signaler immédiatement au responsable IT les alertes concernant les virus.
- Il est formellement interdit de désactiver le programme antivirus.
- Les tests visant à vérifier comment et si le programme antivirus fonctionne en cas de danger sont formellement interdits.

## Accès à Internet uniquement à travers le firewall – aucune chance pour un accès indésirable

**Votre entreprise est-elle équipée de portes coupe-feu? Oui? Vous veillez donc certainement à ce que ces portes soient toujours fermées. Dans le monde d'Internet et de l'échange électronique de données, c'est le firewall qui remplit cette tâche de sécurité. En l'absence de firewall, des personnes qui n'y sont pas autorisées peuvent exécuter des commandes sur votre système informatique, accéder à vos secrets professionnels et aux données soumises à la loi sur la protection des données, mais également exploiter vos ordinateurs pour lancer des attaques illégales vers des tiers.**

- Installez un firewall. Assurez-vous que l'accès à Internet peut être réalisé exclusivement à travers le firewall (voir ci-dessous). Un firewall matériel est recommandé pour les réseaux d'entreprise, alors qu'un firewall logiciel est recommandé pour les appareils mobiles (ordinateurs portables).
- Tous les accès aux réseaux externes doivent être sécurisés par un firewall. Assurez-vous que les connexions avec vos fournisseurs, clients, services externes et collaborateurs qui peuvent accéder à distance à votre réseau, sont sécurisées par des firewalls et que ceux-ci sont mis à jour.
- Certains systèmes d'exploitation, comme Windows XP ou Mac OSX, comportent un firewall intégré, qui n'offre cependant pas une protection complète. Utilisez néanmoins cette possibilité et activez le firewall.
- Si votre entreprise utilise des Wireless-LAN-Computer, assurez-vous que leur utilisation est correcte et sécurisée (voir étape 6). Des appareils Wireless-LAN mal utilisés annihilent l'ensemble de la protection offerte par votre firewall.
- Le firewall doit être régulièrement mis à jour pour les modèles de menaces les plus récents (mises à jour – voir étape 5) et son fonctionnement doit être vérifié.
- Si l'accès à la configuration de votre firewall peut être protégé par un mot de passe, utilisez impérativement cette protection. Utilisez pour cela un mot de passe robuste (voir étape 7). Il est intéressant de sauvegarder la configuration du firewall (voir étape 2).

### Conseils pour les prescriptions IT destinées aux collaboratrices et aux collaborateurs:

Tout le trafic Internet doit être réalisé à travers le firewall. Pour les raisons de sécurité, il est interdit:

- D'accéder à Internet par d'autres moyens, par exemple via un modem,
- D'utiliser des ordinateurs portables privés et des appareils Wireless-LAN dans l'entreprise sans une autorisation écrite du responsable IT.

**Vous contrôlez régulièrement le niveau d'huile et la pression des pneus de votre voiture? Vous faites remplacer à temps les garnitures de freins usées? De même que vous entretenez régulièrement votre voiture pour des raisons de sécurité, vous devez entretenir régulièrement les programmes informatiques de votre entreprise et les maintenir à jour.**

Les personnes font des erreurs – les programmes informatiques sont écrits par des personnes – il n'y a donc pas de programmes informatiques sans erreurs. C'est pour cette raison que les fabricants proposent régulièrement des mises à jour logicielles, appelées «Updates» («mises à jour») ou «Patches» («correctifs»).

- Assurez-vous que les «Patches» les plus récents sont installés pour les systèmes d'exploitation et les applications que vous utilisez.
- Installez les mises à jour pour la version de système d'exploitation (par exemple Windows XP) et pour les versions d'application que vous utilisez effectivement (par exemple Explorer 6).
- Installez systématiquement les «mises à jour de sécurité» disponibles.
- Dans le cas de «mises à jour» qui ne concernent pas la sécurité, il est recommandé de vérifier, en particulier si vous utilisez des programmes de différents fabricants (par exemple Windows et application SAP), si le nouveau «patch» ne risque pas de provoquer des perturbations.
- Tous les ordinateurs raccordés au réseau doivent être «patchés ». Cette remarque s'applique également aux ordinateurs portables et aux appareils des collaboratrices et des collaborateurs externes!
- Établissez pour chaque ordinateur une liste des «Updates» installés.

Vous trouverez ici les «Updates» les plus récents pour les produits courants:

Pour Windows:

[www.windowsupdate.com](http://www.windowsupdate.com)

Pour Office:

[www.officeupdate.com](http://www.officeupdate.com)

**Il faut reconnaître que les téléphones portables, les petits ordinateurs de poche et les ordinateurs portables avec Wireless-LAN sont très pratiques, utiles et élégants. Il serait aujourd'hui pratiquement impossible de s'en passer dans le monde de l'entreprise. S'ils sont mal utilisés, ces appareils représentent cependant un immense risque de sécurité pour chaque entreprise. En particulier s'ils contiennent des données sensibles. Les personnes qui sont obligées pour des raisons professionnelles d'enregistrer des données sensibles sur des appareils mobiles doivent mettre en œuvre des mesures de sécurité spéciales.**

- Veillez à n'enregistrer sur les appareils mobiles que les données effectivement nécessaires.
- Tous les appareils mobiles doivent être protégés par un mot de passe robuste (voir étape 7). En cas de perte ou de vol d'un appareil, des personnes qui n'y sont pas autorisées peuvent sinon facilement accéder à vos données confidentielles.
- Les données sensibles doivent être enregistrées sous forme cryptée sur les ordinateurs portables, pour ne pas tomber entre de mauvaises mains en cas de perte ou de vol d'un appareil. De bons programmes de cryptage sont disponibles dans le commerce et peuvent être téléchargés à partir d'Internet (par exemple PGP – Pretty Good Privacy – [www.pgp.com](http://www.pgp.com)).
- Si un appareil Wireless-LAN est mal configuré, un hacker peut s'introduire en quelques minutes sur votre réseau d'entreprise, au moyen de programmes faciles à utiliser, et ce jusqu'à des distances de 500 m! Il faut être particulièrement prudent si vous ou vos collaborateurs accèdent à votre réseau l'entreprise à partir d'un Access Point (Hot Spot) externe.
- Sur les appareils équipés de Bluetooth (téléphones portables, agenda mobile, ordinateurs de poche), n'activez cette fonction que lorsque vous vous en servez. Le reste du temps, désactivez la fonction Bluetooth. Vous courez sinon le risque de voir votre appareil répondre à votre insu aux requêtes d'autres appareils Bluetooth situés à une distance pouvant aller jusqu'à 100 m.
- N'échangez des données par Bluetooth qu'avec des personnes en qui vous avez confiance.

#### **6 étapes pour une utilisation sûre de Wireless-LAN à l'intérieur et à l'extérieur de l'entreprise:**

- Modifiez le nom attribué par le fabricant à votre réseau sans fil (Service Set ID – SSID). N'utilisez en aucun cas comme nouvelle identification le nom de votre entreprise ou un terme qui permet de deviner votre activité.
- Désactivez la diffusion SSID non ciblée.
- Modifiez le mot de passe standard de vos Access Points. Utilisez un mot de passe robuste (voir étape 7).
- Activez le cryptage de transmission des données sans fil WEP (Wired Equivalent Privacy). Si cela est possible, choisissez un cryptage sur 128 bits. Modifiez la clé WEP attribuée par défaut par le fabricant. Attention: la clé WEP peut être brisée en une à deux heures par des programmes spéciaux de hackers. Il est donc nécessaire de changer régulièrement de clé WEP.
- Utilisez un filtre d'adresses MAC si votre produit comporte cette option.
- Les appareils Wireless-LAN ne doivent être exploités qu'à l'intérieur d'un réseau privé virtuel (Virtual Private Network, VPN). Si vous établissez une connexion avec votre réseau d'entreprises par un Access Point public, ne le faites que par VPN. De nombreux systèmes d'exploitation contiennent déjà un système VPN. Utilisez-le!



N'importe quelle personne qui connaît le mot de passe de votre ordinateur ou de celui de vos collaborateurs et qui se connecte avec ce mot de passe, possède votre identité et dispose de vos autorisations. En volant un mot de passe, des personnes non autorisées peuvent accéder facilement aux informations les plus importantes de votre entreprise. Vous devez donc empêcher le vol d'identité dans votre entreprise. Imposez à vos collaborateurs de n'utiliser que des mots de passe robustes et de les changer régulièrement. Rappelez à toutes vos collaboratrices et à tous vos collaborateurs qu'ils sont responsables des manipulations exécutées sous leur nom d'utilisateur.

- Les mots de passe robustes comportent au moins huit caractères, contiennent des majuscules et des minuscules, des chiffres et des caractères spéciaux.
- Mettez impérativement en place des règles mnémotechniques pour les mots de passe! Au lieu de devoir mémoriser le mot de passe, il suffit de se rappeler d'une phrase secrète, ce qui est beaucoup plus facile. Le mot de passe robuste V2al'€abd6% résulte de la phrase «Voici 2 ans, l'Euro a baissé de 6%». Pour identifier ce mot de passe, un programme de hacker aura besoin d'une bonne soixantaine d'années. Autre exemple: la question «Irons-nous à Paris dans 2 x 7 jours?» correspond au mot de passe robuste lnàPd2x7j?.
- Si vous n'êtes pas certain de la force de votre mot de passe, vous pouvez réaliser un test avec un mot de passe similaire. Conseil: un contrôle de mot de passe est amusant et constitue une bonne méthode pour sensibiliser les collaborateurs. Password-Check: [www.datenschutz.ch](http://www.datenschutz.ch)

**Ne pas oublier:** les mots de passe par défaut configurés par le fabricant sur les appareils, les systèmes d'exploitation et les programmes doivent immédiatement être remplacés par le responsable IT – cahier des charges du responsable IT!



#### Mots de passe interdits:

- Comportant moins de huit caractères.
- Mots et noms que l'on trouve dans les dictionnaires, car ils sont très facilement découverts par les programmes des hackers.
- Noms et dates de naissance de la famille – ils sont faciles à deviner par les collègues ou les connaissances.
- Numéros de sécurité sociale ou de passeport.
- Noms ou termes relatifs à votre hobby.
- Suite de chiffres, de lettres ou de touches comme 1234, abcde, asdf

#### Opérations interdites avec les mots de passe:

- Inscrire des mots de passe sur une fiche (Post-it) ou dans l'ordinateur
- Utiliser le même mot de passe sur une longue période – changer de mot de passe au moins tous les mois ou tous les deux mois (forcer éventuellement le changement de mot de passe par le responsable IT)
- Transmettre un mot de passe à un tiers. Si cela devait arriver malgré tout, changer immédiatement le mot de passe.

## Les prescriptions IT et les campagnes de sécurité garantissent la clarté avec les collaboratrices et les collaborateurs

**Votre entreprise fait-elle partie de celles où «ce qui ne gêne pas est autorisé»? En l'absence de prescriptions de sécurité obligatoires et compréhensibles, vos collaborateurs ne peuvent pas savoir quelles manipulations sont autorisées et lesquelles sont interdites. N'abandonnez pas la sécurité de vos informations et des secrets de votre entreprise au bon vouloir de vos collaborateurs. Cependant, les règles de sécurité sont ressenties par de nombreuses personnes comme une gêne, et sont contournées. Il est donc important de sensibiliser régulièrement vos collaborateurs aux implications de la sécurité dans votre entreprise. Les règles de sécurité ne sont cependant prises au sérieux que si elles sont également respectées par la chef et par le chef. Comportez-vous toujours comme un exemple pour tous les aspects de la sécurité.**

- Etablir par écrit les règles de sécurité et les prescriptions IT, et les faire signer par les collaborateurs (voir ci-dessous).
- Assurer la formation de base de tous les collaborateurs, par exemple en vous appuyant sur cette brochure.  
Objectifs importants:
  - Définition de mots de passe robustes (voir aussi étape 7)
  - Utilisation sûre d'Internet et des e-mails
  - Utilisation sûre des programmes antivirus
  - Enregistrement et sauvegarde des documents
  - Utilisation sûre des appareils mobiles (voir étape 6)
  - Compréhension des règles de sécurité et des prescriptions IT (voir ci-dessous)
- Réaliser chaque année une à deux campagnes de sécurité et de sensibilisation. Ces opérations sont peu coûteuses à réaliser grâce à des moyens simples, par exemple par l'envoi d'un e-mail à chaque collaborateur, par un courrier interne et par des affiches à l'entrée de l'entreprise et à la cantine. Des articles dans le journal de l'entreprise, etc. sont également des moyens très efficaces.
- Faire en sorte que la sécurité dans l'entreprise soit un thème récurrent, dans des occasions diverses.

### Points typiques pour les prescriptions IT destinées aux collaboratrices et aux collaborateurs:

- Définir la manière d'utiliser les mots de passe (voir étape 7)
- Interdire l'utilisation et l'installation de programmes non autorisés (en particulier les jeux, les économiseurs d'écran animés, etc.)
- Interdire l'utilisation de composants matériels non autorisés (par exemple USB-Sticks, modems, ordinateurs portables privés, Wireless-LAN, Handheld-Computer etc.)
- Définir l'utilisation d'Internet – le téléchargement d'information à partir d'Internet est autorisé, mais pas celui de programmes, comme des économiseurs d'écran animés, des films, etc. Interdire la visite de Chatrooms et de sites Web aux contenus pornographiques, raciste ou sexistes.
- Définir l'utilisation des e-mails et l'utilisation des programmes antivirus, y compris leur mise à jour, sauf si elle est réalisée de manière centralisée
- Régler l'utilisation des patches de sécurité, sauf s'ils sont gérés de manière centralisée
- Définir l'utilisation sûre des appareils mobiles (voir étape 6)
- Définir les sauvegardes de données et l'obligation de conservation
- Respecter le système d'organisation prescrit (voir étape 10)
- Régler l'utilisation des données soumises à la loi de protection des données
- Déterminer l'utilisation des informations et des données internes, confidentielles et secrètes – par exemple en définissant des données qui peuvent être diffusées par e-mail
- Régler le comportement en cas d'événements ayant trait à la sécurité, par exemple en cas d'alerte de virus, de perte ou de vol d'ordinateurs portables et de mots de passe – le responsable IT doit immédiatement être informé
- Définir les mesures disciplinaires et les sanctions appliquées en cas d'infraction aux règles de sécurité interne

*Prescriptions destinées aux collaboratrices et aux collaborateurs pour l'utilisation IT*

**Savez-vous qui entre et qui sort de chez vous? Avez-vous une confiance absolue dans tous vos visiteurs? Il suffit de quelques précautions pour éviter que des informations importantes de votre entreprise ne soient détournées au profit de personnes non autorisées, par simple inattention. La sécurité vécue est aujourd'hui un critère de qualité et contribue à la confiance des clients et des fournisseurs.**

- Ne laissez pas de visiteurs, de clients et de connaissances circuler sans surveillance dans votre entreprise.
- Faites chercher à l'accueil et raccompagner à la sortie les personnes externes.
- Si vous ne disposez pas d'un guichet de réception qui peut surveiller l'entrée, ou s'il n'est pas occupé en permanence, prenez la précaution de maintenir la porte d'entrée fermée, et apposez un panneau «Veuillez sonner s.v.p.!»
- Assurez-vous que les clefs et les badges sont gérés correctement et que leur liste est tenue à jour. Ne distribuez que de manière restrictive les clés ayant fonction de passepartout. Vérifiez périodiquement que les autorisations accordées sont justifiées.
- Vérifiez que les collaboratrices et les collaborateurs qui quittent l'entreprise rendent leurs clefs, leurs badges et leurs autorisations d'accès.
- Vérifiez que toutes les portes d'entrée, à l'avant et à l'arrière, ainsi que les fenêtres du rez-de-chaussée sont équipées d'une protection suffisante contre les effractions. Procurez-vous les fiches d'informations correspondantes auprès de la police locale.
- Les serveurs doivent être implantés dans des locaux fermés auxquels seuls le responsable IT et son suppléant ont accès. Si ce n'est pas possible, installer le serveur au moins dans une armoire informatique fermant à clef (rack).
- Ne stockez pas de matériaux inflammables comme du papier dans le local du serveur.
- Assurez-vous qu'un extincteur à CO<sub>2</sub> est placé dans le local du serveur ou à sa proximité immédiate.
- Les imprimantes réseau ne doivent pas être installées dans des locaux accessibles au public, car des personnes non autorisées pourraient consulter les documents qui ne leur sont pas destinés (loi sur la protection des données, secrets d'entreprise, etc.).
- Les câbles réseau qui traversent des locaux accessibles au public, ainsi que les modems, les routeurs et les autres équipements de réseau placés dans des locaux publics, doivent être spécialement protégés.

**L'ordre a-t-il quelque chose à voir avec la sécurité? Certainement plus qu'il n'apparaît au premier coup d'œil. Indépendamment du temps que l'on peut gagner grâce à une table de travail rangée, on perd moins d'informations et de documents que si la table de travail est encombrée de papiers, de fiches et de dossiers. On peut également diminuer ainsi le risque de voir des documents sensibles apparaître à un moment inapproprié, ou être lus par hasard par des personnes non autorisées. L'ordre contribue également à l'image de votre entreprise: les clients ou les fournisseurs tirent facilement des conclusions sur le fonctionnement interne de l'entreprise en se basant sur ce qu'ils peuvent en voir.**

- Mettre en place pour les données électroniques et les documents papier un système de classement que tout le monde doit respecter – par exemple par client, par projet, etc.
- Le système de classement doit être structuré de manière logique et être conçu pour être bien compris par les collaboratrices et les collaborateurs, et donc être bien appliqué (voir étape 8).
- La transmission bien organisée des tâches et des documents pendant les périodes de vacances évite que des collaborateurs ne puissent fouiller dans les documents ou les ordinateurs de leurs collègues, et consulter par hasard des informations qui ne leur sont pas destinées.
- Mettre en place les bases d'une meilleure sécurité, sous forme d'un nombre suffisant d'armoires, de coffres, de dossiers, etc.
- Pendant les pauses ou les absences du poste de travail, l'ordinateur doit être éteint ou un économiseur d'écran doit être activé avec mot de passe, pour que les personnes non autorisées ne puissent consulter les documents en cours de traitement. Si vous travaillez avec les données sensibles, fermez votre bureau à clef.
- Détruire les documents et les notes sur papier contenant des données sensibles, dès qu'ils ne sont plus nécessaires. Ils ne doivent pas être jetés dans une corbeille à papiers, ni à la poubelle.
- Les données électroniques qui ne sont plus nécessaires et qui sont enregistrées sur des supports comme des disquettes, des CD ou des DVD, doivent être effacées de manière sûre et écrasées plusieurs fois. Ce n'est pas possible sous Microsoft-Windows. La simple commande d'effacement ne suffit pas! Il est donc nécessaire de détruire physiquement les supports de données qui ne sont plus nécessaires s'ils contiennent des données sensibles.
- Si l'on donne des supports de données qui doivent sortir de l'entreprise, il faut utiliser des supports neufs et non encore utilisés. Les informations effacées de manière conventionnelle sont faciles à reconstituer et peuvent être lues par des personnes non autorisées.
- Les dossiers contenant des données personnelles, des contrats et des offres doivent être conservés sous clef, pour éviter toute infraction à la loi sur la protection des données.
- Les personnes qui travaillent sur leur ordinateur avec des données sensibles doivent orienter leur écran de manière à ce que les collègues et les visiteurs ne puissent pas lire les informations.

# Glossaire

**Adresse IP** Adresse numérique permettant d'identifier chaque appareil dans un réseau.

**ADSL** Accès Internet très rapide. Avec l'ADSL, l'ordinateur ou le serveur est connecté en permanence à Internet, et est donc exposé en permanence aux attaques des hackers – mettre en œuvre un *firewall*!

**Application** Programme d'utilisation, par exemple traitement de texte ou programme d'e-mail.

**Attachment** Fichier joint à un e-mail. De nombreux programmes malicieux (*Malicious Code*) sont diffusés par des fichiers joints et sont activés lors de leur ouverture. Il ne faut donc ouvrir que les fichiers joints envoyés par des expéditeurs connus.

**Backup** Sauvegarde de données, de programmes et de configuration de programmes.

**Browser** Programme qui permet de consulter des informations sur des serveurs sur Internet.

**CD** Support de données présentant une capacité allant jusqu'à 700 Mb.

**Client** Poste de travail, c'est-à-dire ordinateur isolé connecté au réseau.

**Disquette** Support de données présentant une capacité de 1,44 Mb, non adapté à la conservation de données à long terme.

**Download** Littéralement «téléchargement», désigne le chargement de programmes et de mises à jour à partir d'Internet.

**DVD** Support de données présentant une capacité de 4,3 Gb.

**Firewall** Littéralement «mur pare-feu», appareil ou programme de sécurité qui sécurise la connexion à Internet et protège un réseau ou un ordinateur isolé contre les accès non autorisés à partir de l'extérieur du réseau.

**Hub** Appareil auquel plusieurs ordinateurs d'un réseau sont raccordés, pour réaliser une topologie structurée en forme d'étoile.

**ISDN** Réseau de télécommunication numérique pour la transmission de téléphonie, de télécopies et des données avec une vitesse de transmission de 64 ou de 128 kbits par seconde. Comparé aux techniques analogiques, offre une meilleure qualité de transmission et une meilleure sécurité.

**Junk-Mail** Littéralement e-mail poubelle, désigne des e-mails non désirés.

**Logiciels** Informations et programmes qui peuvent être traités ou exécutés par le *Hardware*.

**Login** Connexion à un service, généralement au moyen d'un nom d'utilisateur et d'un mot de passe.

**Malicious Code** Terme générique désignant des programmes malicieux, par exemple des *virus*, des *vers*, des *chevaux de Troie*, etc.

**Matériel (Hardware)** Appareil physique, par exemple ordinateur, imprimante, souris, clavier, etc.

**Modem** Système électronique utilisé pour la préparation et/ou la conversion des signaux électriques pour l'envoi et la réception sur les réseaux de communication, permettant l'accès à Internet à travers les lignes téléphoniques.

**Mot de passe** Code d'identification secret ou clef secrète.

**Nom d'utilisateur** Pour permettre la connexion à un programme ou à un service (par exemple Internet), il faut généralement donner un nom d'utilisateur et un *mot de passe*. Ces informations permettent d'identifier les utilisateurs autorisés.

**Patch** Littéralement pansement, mise à jour de système d'exploitation ou de programmes utilisateur (*Update*).

**Port** Indication numérique permettant de conduire un paquet de don-

nées reçu à bon port, c'est-à-dire de le transmettre au service approprié. C'est ainsi qu'un e-mail entrant est identifié comme tel et transmis au programme d'e-mail.

**Provider** Fournisseur d'accès à Internet, par exemple Bluewin, Sunrise, Cablecom, Green.ch, etc.

**Remote Access** Accès à distance au réseau d'entreprise. Les autorisations pour le Remote Access doivent être limitées dans le temps, et les activités des personnes autorisées à utiliser le Remote Access doivent être surveillées.

**Routeur** Appareil servant à relier entre eux plusieurs réseaux.

**Scanner antivirus** Programme de détection des *virus* informatiques.

**Serveur** Ordinateur donnant accès à ses ressources matérielles et logicielles dans un réseau à d'autres ordinateurs (*Clients*), par exemple serveur d'applications, serveur de fichiers, serveur d'e-mail, serveur Web.

**Signature numérique** Signature numérique ayant valeur d'engagement.

**Spam** e-mail en masse, comparable aux chaînes de lettres qui étaient envoyées par la poste. Ils peuvent être interceptés par un *Spamfilter*.

**Spamfilter** Programme filtrant les *Spam*-e-mails de la boîte de réception. Les fournisseurs d'accès à Internet offrent souvent la possibilité de filtrer les Spam à leur niveau, pour éviter que des e-mails indésirables n'encombrent régulièrement les boîtes de réception. Des programmes sont disponibles dans le commerce et offrent une protection plus complète contre les Spam. Plusieurs fabricants proposent des ensembles de programmes qui regroupent un firewall, un antivirus et un Spamfilter.

**Switch** Appareil servant à relier entre eux plusieurs ordinateurs.

**Système d'exploitation** *Logiciel* ou programme système. Ensemble de programmes généralement petits, chargés au démarrage de l'ordinateur et nécessaires à son fonctionnement.

**Troyen, cheval de Troie** Partie malicieuse d'un programme (*Malicious Code*). Transmis généralement comme composant d'un e-mail, lors du chargement d'un fichier ou à travers un port resté ouvert sur l'ordinateur. Ces programmes s'activent dans des conditions prédéfinies sur l'ordinateur infecté et collectent, manipulent ou détruisent des données. Forme moderne d'espionnage et de sabotage.

**Update** Mise à jour d'un programme (*Patch*).

**URL** Adresse d'une page sur Internet, par exemple [www.infosurance.ch](http://www.infosurance.ch).

**USB-Stick** Support de mémoire qui se branche sur le port USB. Grâce à sa petite taille et à sa grande capacité (jusqu'à 1 Gb), appareil volontiers mis en œuvre dans le cadre de l'espionnage industriel.

**Virus** Programme malicieux et caché (*Malicious Code*), qui détruit des données. Il peut être transmis et diffusé par toutes les formes de transmission de données (Internet, disquettes, CD, réseau, etc.) – Mettre en œuvre un programme antivirus.

**VPN** Abréviation de Virtual Private Network (réseau privé virtuel). Réseau établi à travers une connexion virtuelle (par exemple via Internet) pour transmettre des données de manière sécurisée (cryptées). Grâce à un réseau VPN, les différentes filiales d'une entreprise peuvent communiquer entre elles économiquement et en toute sécurité.

**Ver** Programme malicieux (*Malicious Code*) indépendant d'un fichier, qui exploite les lacunes de sécurité pour se diffuser d'un ordinateur à l'autre et d'un réseau à l'autre par copie. Généralement, les vers contiennent des commandes qui détruisent directement des données ou qui réduisent les performances des systèmes.

**Zombie** Ordinateur télécommandé utilisé typiquement pour des attaques concentrées sur Internet.

Nous remercions les personnes et les institutions citées ci-après pour leur engagement, l'apport de leur savoir-faire et pour les documents de base élaborés dans le groupe spécialisé PME de la Fondation InfoSurance au cours d'un grand nombre d'heures de travail d'intérêt général:

Carlos Rieder, Hochschule für Wirtschaft, Lucerne (responsable du groupe spécialisé PME de la Fondation InfoSurance)

Jürg Altenburger, IBM , Zurich

Christoph Bangerter, E-Mediat AG, Schönbühl

Marcel Beil, Symantec Switzerland AG, Bassersdorf

Herbert Brun, UPAQ Ltd, Küsnacht

Roger Caspar, Bluewin, Zurich

Martin Denz, Association des médecins suisses FMH, Berne

Christof Egli, Ernst Basler + Partner AG, Zollikon

Roger Halbheer, Microsoft Schweiz GmbH, Wallisellen

Peter Kunz, Omnisec, Dällikon

Anton Lagger, Office fédéral de l'économie, Berne

Peter Neuhaus, Fondation PME Suisse, Berne

Peter Otth, Symantec Switzerland AG, Bassersdorf

Ivo Pfister, Fondation InfoSurance, Zurich

Marc Vallotton, InfoGuard AG, Zug

Christian Weber, Secrétariat d'État à l'économie SECO, Berne

