suissetec

Schweizerisch-Liechtensteinischer Gebäudetechnikverband
Association suisse et liechtensteinoise de la technique du bâtiment
Associazione svizzera e del Liechtenstein della tecnica della costruzione
Associaziun svizra e liechtensteinaisa da la tecnica da construcziun

Janvier 2018

Notice technique

Sécurité informatique pour les PME

Plus de sécurité pour les systèmes informatiques des petites et moyennes entreprises (PME)
Une protection accrue grâce au programme en 10 points de l'association ISSS

Introduction

La Suisse compte parmi les principaux utilisateurs de technologies de l'information et de la communication (TIC) dans le monde. Personne ne dépense autant d'argent par habitant pour les technologies informatiques que les Suisses. Plus rien ne fonctionne sans l'informatique.
Le présent aide-mémoire a été conçu pour les PME suisses, afin de les aider à accroître la sécurité informatique de leurs réseaux d'entreprise. Le Programme en dix points se veut compréhensible et peu onéreux dans sa mise en oeuvre. Mais pour tous les cas où des connaissances spécifiques s'avèrent nécessaires, n'hésitez pas à vous adresser à un expert.
Nous tenons à souligner qu'à elles seules, les mesures techniques ne suffisent pas à garantir la sécurité informatique d'un réseau d'entreprise. Des mesures organisationnelles s'avèrent également à chaque fois nécessaires. Dans le cas des mesures onéreuses ou mobilisant d'importantes ressources, chaque entreprise, plus précisément sa direction, doit trouver un juste équilibre entre le coût d'une telle mesure et les risques encourus en ne la réalisant pas. Autrement dit, la direction doit décider soit de supporter les risques en question, soit de fournir les ressources utiles pour les réduire au minimum.

Le programme en 10 points : vue d'ensemble

10 mesures pour une protection de base efficace

1. Etablissez un cahier des charges pour les responsables informatiques !
2. Protégez vos données en faisant régulièrement des backups
3. Effectuez toujours les dernières mises à jour de votre antivirus !
4. Protégez votre navigation sur Internet avec un parefeu
5. Effectuez régulièrement les mises à jour de vos logiciels !
6. Choisissez des mots de passe complexes !
7. Protégez vos appareils portables !
8. Expliquez vos directives pour l'utilisation des moyens informatiques !
9. Protégez l'environnement de vos infrastructures informatiques !
10. Adoptez un bon système de classement pour vos documents et dossiers

1

Etablissez un cahier des charges pour les responsables informatiques !

Principes

La sécurité informatique repose sur des facteurs techniques, humains et organisationnels !

Des solutions techniques en matière de sécurité et des collaborateurs motivés, c'est bien ! Mais la direction doit elle aussi contribuer activement pour garantir une protection de base efficace.

Notes :

- Toute entreprise a besoin d'un responsable informatique et de son remplaçant. Les connaissances nécessaires pour occuper un tel poste peuvent être acquises lors d'une formation spécialisée. Il arrive aussi souvent que les petites entreprises fassent appel à des spécialistes externes. Pour l'entreprise, cela représente bien sûr un coût, mais bien moindre comparé aux conséquences d'une perte des données ou de la violation de la loi sur la protection des données.
- La direction délègue officiellement les questions de sécurité au responsable informatique et définit ses tâches dans un cahier des charges (cf. cidessous).

Trucs et astuces :

- Sauvegardez régulièrement vos données sur des serveurs, stations de travail, notebooks et autres appareils portables (cf. point n 2).
- Effectuez les dernières mises à jour de vos systèmes d'exploitation, programmes antivirus, pare-feux et autres logiciels (cf. points n 3, 4 et 5).
- Modifiez immédiatement les réglages de mots de passe internes sur les ordinateurs, systèmes d'exploitation et programmes d'application.
- Etablissez une liste de tous les ordinateurs de l'entreprise en précisant les programmes installés et les mises à jour effectuées (cf. point n 5).
- La direction vérifie que le responsable informatique s'acquitte correctement de sa tâche.
- Tous les collaborateurs qui travaillent sur ordinateur doivent recevoir un guide contenant les directives pour l'utilisation des moyens informatiques. Ces directives décrivent les opérations que vos collaborateurs sont autorisés ou non à effectuer sur l'ordinateur (cf. point n°8).
- Désignez un interlocuteur pour toutes les questions liées à la sécurité : perte d'un ordinateur portable par exemple ou infection par un virus, etc.
- Déterminez les droits d'accès de vos collaborateurs aux différents programmes et données.
- Etablissez une liste de toutes les personnes habilitées à accéder de l'extérieur au réseau de l'entreprise, en indiquant le cas échéant la durée précise de leurs droits. Assurez-vous que les programmes de protection sont régulièrement mis à jour.
- Veillez au respect des mesures de sécurisation des données, à travers par exemple des programmes de protection et des mots de passe complexes (cf. points n 3, 4, 6).
- Contrôlez régulièrement la bonne application desdirectives contenues dans le guide informatique.

2

Protégez vos données en faisant régulièrement des backups !

Principes

Il existe différentes manières de perdre des données : elles peuvent être écrasées par erreur, rendues illisibles à cause d'un défaut sur le disque dur, voire détruites par un incendie ou un dégât des eaux.
Vous pouvez éviter de tels désagréments en faisant régulièrement des backups de vos données.

Notes :

- En règle générale, il convient d'effectuer des backups de sécurité pour toutes les données dont le contenu est vital pour la poursuite de votre activité. De même, les configurations de logiciels devraient également faire l'objet de sauvegardes.
- La fréquence de ces backups dépend de l'activité et de la taille de votre entreprise. Ceci dit, une PME devrait sauve-garder ses données au moins une fois par semaine.
- Un backup quotidien vous permet de réaliser un archivage de vos données conforme au droit des obligations et à l'ordonnance concernant la tenue et la conservation des livres de comptes (Olico) (cf. ci- dessous).

Trucs et astuces :

- Du lundi au jeudi, effectuez un backup quotidien sur différents supports de stockage. La semaine suivante, procédez de la même manière en écrasant les données des précédents backups jour après jour. Conservez les backups journaliers en dehors du local où se trouve votre serveur.
- Chaque vendredi, faites un backup pour la semaine écoulée sur un support de stockage différent que vous conserverez hors de l'entreprise. Les backups hebdomadaires seront écrasés au bout d'un mois.
- Désignez par écrit les responsables des sauvegardes de sécurité et établissez une liste des backups effectués.
- Sauvegardez toujours vos données sur des supports mobiles (bande magnétique et autres supports amovibles).
- De même, il serait bon d'effectuer des copies des documents importants dont vous ne disposez que d'une version papier (contrats ou autres) et de les conserver hors de l'entreprise.
- Attention ! Certains documents comme les bilans, les comptes de résultats, les livres de comptes, les inventaires, les justificatifs comptables et la correspondance commerciale doivent être conservés pendant 10 ans.
- A la fin du mois, faites un backup pour le mois écoulé. Cette sauvegarde de sécurité mensuelle ne sera pas écrasée et devra être conservée hors de l'entreprise.
- A la fin de l'année, faites un backup de l'année écoulée. Cette sauvegarde de sécurité annuelle ne sera pas écrasée et devra être conservée elle aussi hors de l'entreprise
- Vérifiez régulièrement que les données sauvegardées sur les supports de stockage sont accessibles. Une sauvegarde n'a de sens que si les données ont été correctement copiées sur le support.

3

Effectuez toujours les dernières mises à jour de votre antivirus !

Principes
Des programmes nuisibles, tels que par exemple les virus et les vers, peuvent paralyser vos infrastructures informatiques et mettre ainsi la vie de votre entreprise en péril.

Notes :
- Les virus informatiques peuvent modifier, corrompre, voire même détruire complètement données et programmes. Ces programmes malveillants peuvent vous être transmis en pièce jointe d'un email, par messagerie instantanée, etc. Sur Internet, ces virus sont souvent déguisés en programmes gratuits, pseudoutiles ou de divertissement et s'activent en un simple clic de souris.
- Les systèmes informatiques mal protégés sont souvent pervertis pour propager des virus et pour lancer des attaques ciblées contre une société tierce. Un chef d'entreprise qui ne prend pas les mesures suffisantes pour protéger ses systèmes informatiques fait preuve de négligence et s'expose à des poursuites pénales.

Trucs et astuces :
- Installez un programme antivirus sur tous les serveurs, postes de travail (clients) et ordinateurs portables, et effectuez régulièrement les mises à jour (une fois par jour minimum).
- Interdisez expressément la désactivation, même temporaire, du programme antivirus
- Demandez à vos collaborateurs de signaler immédiatement au responsable informatique les messages d'avertissement virus.
- Un programme antivirus offre une protection contre les virus et les vers connus. Il identifie les intrus et les met hors d'état de nuire. Ces programmes sont en vente dans les magasins d'informatique mais on en trouve aussi en téléchargement gratuit sur la toile.
- Les cybercriminels ne cessent de mettre au point de nouveaux virus, raison pour laquelle il convient d'actualiser continuellement votre programme antivirus. Selon le produit utilisé, le programme recherche lui-même les mises à jour sur la page d'accueil du fabricant. Demandez à votre vendeur si c'est le cas pour votre antivirus. Quoiqu'il en soit, les mises à jour doivent être effectuées chaque jour.
- Effectuez au moins une fois par semaine un scan complet de votre disque dur. Vous pourrez ainsi découvrir et éliminer des virus qui n'avaient pas encore été détectés.
- Interdisez expressément tout test «maison» sur les virus.
- Pour les réseaux d'une certaine importance, les mises à jour des antivirus doivent se faire de façon centralisée et automatique.

4

Protégez votre navigation sur Internet avec un pare-feu !

Principes
Si vous avez des portes coupe-feu dans votre entreprise, vous veillez certainement à ce qu'elles soient toujours bien fermées. Dans le monde de l'Internet et de l'échange électronique de données, c'est le pare-feu qui remplit cette fonction sécuritaire.

Notes :
- En l'absence de pare-feu, n'importe qui peut s'immiscer dans votre système informatique, exécuter des taches à votre insu, utiliser votre ordinateur pour lancer des attaques illégales contre des tiers, ou bien encore accéder à des données commerciales confidentielles relevant de la loi sur la protection des données.
- Pour les réseaux d'entreprise d'une certaine taille, il est recommandé d'adopter un pare-feu autonome (appareil spécial) ainsi qu'un pare-feu intégré (dans le système lui-même) pour les différents ordinateurs fixes et portables.
- Vous trouverez dans le commerce des produits faisant à la fois office de parefeu et d'antivirus. Ces produits combinés sont particulièrement indiquées pour les petites entreprises.

Trucs et astuces :
- Installez un pare-feu et effectuez régulièrement les mises à jour.
- Tout le trafic Internet doit passer à travers le crible du pare-feu. N'autorisez aucun autre accès à Internet (par ex. via modem).
- N'utilisez aucun ordinateur portable ou réseau local sans fil privé sans l'autorisation écrite du responsable informatique.
- Plusieurs systèmes d'exploitation disposent d'un pare-feu intégré. Profitez systématiquement de cette possibilité et activez ces pare-feux.
- Si vous utilisez un réseau local sans fil (WLAN) dans votre entreprise, veillez à ce qu'il soit sûr et sécurisé. Un réseau local sans fil mal configuré anéantit toute la protection offerte par le système de pare-feu.
- Toutes les passerelles réseau doivent être sécurisées par un pare-feu. Toutes les connexions entre fournisseurs, clients, sous- traitants et collaborateurs (même en accès à distance) et votre réseau doivent être contrôlées par un pare-feu.
- Protégez la configuration de votre pare-feu avec un mot de passe complexe
- Sauvegardez régulièrement la configuration du pare-feu central.

5

Effectuez régulièrement les mises à jour de vos logiciels !

Principes

Contrôlez-vous régulièrement le niveau d'huile et la pression des pneus de votre voiture ? C'est souhaitable.
De la même manière que vous entretenez régulièrement votre voiture, vous devez veiller à ce que les programmes informatiques de votre entreprise soient régulièrement mis à jour pour être toujours au top niveau.

Notes :

- Les logiciels actuels contiennent souvent des millions de lignes codées. Or malgré les contrôles, il arrive parfois qu'une erreur se faufile à travers ces lignes. Pour un fabricant, il est pratiquement impossible de tester chaque application dans tous les environnements et configurations possibles. C'est pourquoi les fabricants proposent régulièrement des patchs correctifs qui permettent de rattraper les erreurs connues.
- Si vous ne mettez pas à jour régulièrement vos programmes, des cybercriminels peuvent exploiter des failles connues pour manipuler des données ou abuser de votre infrastructure à des fins peu scrupuleuses.
- La plupart du temps, les systèmes d'exploitation et les applications sont en mesure de télécharger automatiquement les mises à jour sur Internet. Les sites Internet des fabricants de logiciels et le manuel d'utilisation vous fourniront à ce sujet une aide utile.

Trucs et astuces :

- Installez les tout derniers patchs correctifs de vos systèmes d'exploitation et applications.
- Installez dès que possible les mises à jour de sécurité disponibles.
- Installez les mises à jour uniquement pour les versions des logiciels que vous utilisez.
- Soyez le moins vulnérable possible et n'installez donc que les programmes dont vous avez vraiment besoin et désactivez les services, validations de réseaux et autres protocoles inutiles. Ce qui n'existe pas ne peut être piraté et ne nécessite pas de maintenance !
- Si vous-même découvrez des points faibles ou si le logiciel répond de façon inattendue, il convient d'en informer le fabricant.
- Installez les patchs sur tous les ordinateurs fixes et portables, y compris ceux de vos collaborateurs externes !
- Etablissez une liste pour recenser quelles mises à jour ont été installées et sur quel ordinateur.

Pour télécharger les toutes dernières mises à jour des produits Microsoft : www.windowsupdate.com

6

Choisissez des mots de passe compliqués !

Principes

Il suffit de connaître le nom et le mot de passe d'un utilisateur pour se connecter dans un système à sa place et abuser de son identité (informatique !) et de tous ses droits d'accès.
Le vol de mots de passe permet aux cyberpirates d'accéder, à peu de frais, à des informations commerciales confidentielles. Faites en sorte qu'on ne puisse usurper des identités au sein de votre entreprise

Notes :

- Les mots de passe permettant d'accéder aux ordinateurs, systèmes d'exploitation et applications de votre entreprise doivent être modifiés immédiatement par le responsable informatique (cf. point n 1).
- Invitez vos collaborateurs à choisir des mots de passe compliqués qu'ils devront changer régulièrement. Ils doivent être conscients du fait qu'ils seront tenus responsables des actions commises sous leur nom d'utilisateur.
- Les mots de passe complexe sont composés d'au moins 9 caractères, dont des majuscules, des minuscules, des chiffres et des caractères spéciaux.

Trucs et astuces :

- N'utilisez aucun mot de passe pouvant se trouver dans un dictionnaire.
- N'utilisez pas de mots de passe contenant des le nom, le numéro de passeport ou d'AVS, ou la date de naissance d'un de vos proches.
- Contrôler le niveau de sécurité de votre mot de passe avec un testeur de mots de passe.
- Voici comment créer un mot de passe compliqué :
  Exemple n°1 : prenez un mot simple comme «nuage», intercalez un caractère spécial, introduisez des majuscules et complétez par un chiffre correspondant au mois courant. Vous obtenez ainsi un mot de passe complexe «Nu$aGe04».
  Exemple n°2 : à partir d'une phrase comme «Nous avons passé deux jours à Paris !», vous pouvez tirer le mot de passe «Nap2jàP !» en mettant à la suite la première lettre de chaque mot et les chiffres. Il sera plus facile de mémoriser une phrase qui a du sens plutôt qu'un mot de passe cryptique !
- N'écrivez jamais vos mots de passe sur un bout de papier, à moins de le conserver sous clé ! Beaucoup d'utilisateurs laissent leurs mots de passe dans un rayon d'un mètre de leur ordinateur.
- Ne communiquez jamais votre mot de passe à des tiers. Une personne peut être remplacée sans qu'elle doive nécessairement révéler son mot de passe. Si vous constatez qu'un tiers connaît votre mot de passe, modifiez-le immédiatement.

Pour vérifier le niveau de sécurité de votre mot de passe : https ://passwortcheck.datenschutz.ch/

7

Protégez vos appareils portables !

Principes

Les téléphones mobiles, ordinateurs portables et assistants personnels en connexion WLAN sont à la fois pratiques et multitâches.

Mal employés, ces appareils représentent cependant un risque important. Aussi, quiconque est tenu, pour des raisons professionnelles, de stocker des données sensibles sur un appareil portable, doit prendre des mesures spéciales.

Notes :

- Tous les ordinateurs portables doivent être protégés par un mot de passe compliqué (cf. point n 6).Sinon, n'importe qui pourrait accéder aux données commerciales de votre entreprise en cas de perte ou de vol d'un portable.
- Les appareils portables ne devraient contenir que les données strictement nécessaires à leur fonction. N'oubliez pas d'effectuer régulièrement un backup de ces données (cf. point n 2).
- Les données sensibles stockées sur un ordinateur portable doivent être protégées par un code d'accès pour éviter qu'elles ne puissent être exploitées par des personnes malintentionnées. Vous trouverez de bons programmes de cryptage dans le commerce, mais aussi en téléchargement sur Internet.

Trucs et astuces :

- Modifiez le nom attribué par le fabricant au réseau local de connexion sans fil (Service Set ID – SSID). Le nouveau nom de devra en aucun cas contenir le nom de votre entreprise.
- Désactiver l'émission SSID pour que votre point d'accès ne soit pas visible à des tiers.
- Activez le cryptage du transfert de données sans fil (WPA2, Wi-Fi Protected Access 2). Modifiez le mot de passe standard de vos points d'accès.
- Les appareils portables doivent être passés régulièrement à l'antivirus, car ils sont synchronisés avec les autres ordinateurs de l'entreprise, à travers les fonctions de messagerie électronique par exemple.
- Une connexion WLAN mal configurée peut permettre aux cybercriminels de s'immiscer, en quelques minutes et jusqu'à une distance d'un kilomètre, dans le réseau de votre entreprise. Il convient de réglementer tout particulièrement l'utilisation de points d'accès publics et externes à Internet (HotSpots).
- Activez le Bluetooth sur vos appareils (téléphones et ordinateurs portables, PC de poche) uniquement en cas de besoin et à l'abri des regards indiscrets. Autrement, votre appareil peut réagir à votre insu à des sollicitations étrangères (dans un rayon allant jusqu'à 100 mètres).
- Utilisez le filtre d'adresses MAC pour que seuls les appareils connus puissent communiquer avec le point d'accès.
- Pour acheminer des données ultraconfidentielles, utilisez exclusivement des connexions protégées par un réseau privé virtuel (VPN).
- Pour crypter ou chiffrer vos données, vous pouvez utiliser le produit Pretty Good Privacy (PGP). Les packages de solutions PGP pour les entreprises sont disponibles sur le site officiel.

https ://www.symantec.com/fr/fr/products/encryption

8

Expliquez vos directives pour l'utilisation des moyens informatiques !

Principes

Sans directives claires et contraignantes, vos collaborateurs ne savent pas ce qu'ils ont le droit de faire et de ne pas faire en tant qu'utilisateur informatique.
Mais les règles ne sont véritablement prises au sérieux que si elles sont respectées par les supérieurs. Vous devez donc servir d'exemple pour tous les aspects liés à la sécurité.

Notes :

- Formulez par écrit les directives pour l'utilisation des moyens informatiques et faites-les signer par vos collaborateurs.
- Abordez régulièrement le problème de la sécurité dans votre entreprise en multipliant les approches.
- Organisez des campagnes de sensibilisation sur ce thème une à deux fois par an. C'est facile à réaliser et cela nécessite très peu de moyens : courriels à tous vos collaborateurs, circulaires internes, affichage à la cantine, articles dans le journal de l'entreprise, etc.

Trucs et astuces :

- Réglementez l'installation et l'utilisation de programmes et matériel n'appartenant pas à la sphère de l'entreprise (jeux, économiseur d'écran, clés USB, modems, ordinateurs portables privés, connexions LAN sans fil, assistants personnels, etc.)
- Réglementez la navigation sur Internet et définissez ce que vos collaborateurs peuvent ou non télécharger (informations, programmes, etc.)
- Interdisez la fréquentation des salons de discussions (chatrooms) et la consultation de sites aux contenus pornographiques, racistes ou violents.
- Définissez le mode de sauvegarde des données, en particulier pour les utilisateurs d'ordinateurs portables (cf. Point n 2).
- Organisez une formation de base pour tous vos collaborateurs (en vous inspirant de cette brochure par exemple). Objectifs :
  - avantages de la sécurité informatique
  - création de mots de passe compliqués
  - pratique sécurisée d'Internet et de la messagerie électronique
  - utilisation de l'antivirus
  - classement des documents
- La version papier ne suffit pas ! Vos collaborateurs doivent être régulièrement sensibilisés au problème de la sécurité.
- Imposez la création de mots de passe. (cf. point n 6).
- Réglementez la gestion des mises à jour de sécurité et des logiciels antivirus (cf. points n 3 et 5).
- Réglementez l'utilisation de la messagerie électronique. Interdiction de transmettre des données confidentielles, de transférer des messages sur les boîtes de messagerie privées, de diffuser les chaînes de lettres etc.
- Définissez le mode de gestion des données et informations confidentielles et organisez un archivage sécurisé de vos fichiers.
- Définissez la procédure à suivre en cas d'incident lié à la sécurité (ex : alertes virus, vol ou perte d'appareils portables ou de mots de passe).

9

Protégez l'environnement de vos infrastructures informatiques !

Principes

Savez-vous qui entre et qui sort de votre entreprise chaque jour ? Quelques dispositions suffisent pour éviter que n'importe qui puisse accéder à des informations commerciales importantes.

Un système de sécurité visible est aujourd'hui un critère de qualité qui ne manquera pas d'inspirer confiance à vos clients et à vos fournisseurs. A quoi bon s'équiper du meilleur pare-feu, si des inconnus peuvent s'introduire dans vos bureaux ?

Notes :

- Tous les accès à vos locaux et au site de votre entreprise doivent être fermés ou surveillés. Si cela n'est pas possible, limitez-vous à la partie bureaux.
- Ne permettez pas aux visiteurs, clients et connaissances de circuler sans surveillance dans votre entreprise.
- Toute personne tierce à l'entreprise doit être accueillie à la réception, accompagnée pendant toute la durée de sa visite et raccompagnée jusqu'à la sortie.
- Si vous n'avez pas de réception permettant de surveiller l'accès, il convient de verrouiller la porte d'entrée et d'apposer une plaque «Prière de sonner».

Trucs et astuces :

- Installez votre serveur dans un local climatisé et fermant à clé. Si cela n'est pas possible, enfermez le serveur dans un caisson (rack).
- N'entreposez pas d'objets inflammables (papier par exemple) ni dans le local du serveur, ni à proximité.
- Placez un extincteur au CO_2 dans le local du serveur en veillant à ce qu'il soit bien en vue.
- Assurez-vous que toutes les ouvertures (fenêtres, portes, etc.) disposent d'un système de protection efficace contre les effractions. Vous trouverez des brochures d'information à ce sujet dans les postes de police.
- Clés et badges doivent être correctement gérés et leur listes mises à jour. Soyez parcimonieux dans la distribution des clés passe-partout qu'il convient de réexaminer au moins une fois par an.
- Les collaborateurs qui quittent définitivement l'entreprise doivent remettre leurs clés, badges et autres droits d'accès.
- Ne placez pas d'imprimante réseau dans des pièces accessibles au public pour protéger vos documents des regards indiscrets.
- Enfermez les câbles de connexion réseau qui traversent les pièces accessibles au public. Même chose pour vos modems, stations centrales (hubs), routeurs et commutateurs.

10

Classez vos documents et vos dossiers !

Principes

Cela peut paraître surprenant au premier abord, mais ordre et sécurité vont de pair. On perd moins de documents sur un bureau bien rangé.

C'est la même chose pour votre ordinateur et vous éviterez de perdre des données en établissant un système de classement bien ordonné.

Notes :

- Une méthode de rangement rationnelle permet de réduire le risque, de voir des documents sensibles ressurgir au mauvais moment ou être exposés par hasard à des regards indiscrets.
- Un espace bien rangé est aussi une question d'image : vos clients et vos fournisseurs seront sensibles aux apparences et des bureaux bien rangés leur donneront l'idée d'une gestion ordonnée.
- Classez vos fichiers électroniques et vos documents papier selon la même logique de rangement, par exemple par client ou par projet. Le système doit avoir une structure logique et compréhensible pour vos collaborateurs.

Trucs et astuces :

- Effacez des différents supports de stockage (CD-Rom, DVD, clés USB, disques durs) les données électroniques dont vous n'avez plus besoin en écrasant l'ensemble de l'espace mémoire. La commande «Supprimer» ne suffit pas ! Le mieux est de détruire physiquement ces supports avant de vous en débarrasser.
- Les documents confidentiels (contenant par exemple des données personnelles) doivent être conservés systématiquement sous clé.
- Lorsque vous faites sortir des données de votre entreprise, utilisez des supports de stockage neufs n'ayant encore jamais servi, car il est relativement facile de rétablir des fichiers supprimés de façon conventionnelle. Mieux vaut donc se prémunir des regards indiscrets. Actuellement, seul le programme «Wipe» est en mesure d'effacer définitivement vos données. Vous trouverez sur Internet toutes les informations concernant ce logiciel.
- Lorsque vous travaillez à l'ordinateur sur des données sensibles, positionnez votre écran de sorte que vos collègues ou des visiteurs ne puissent pas lire ce qui y est affiché.
- Détruisez les documents sur support papier dont vous n'avez plus besoin, de même que les notes contenant des données sensibles (destructeur de documents).
- Pendant les pauses ou en cas d'absence, verrouillez l'accès de votre ordinateur par un mot de passe et mettez vos documents confidentiels sous clé.
- Ne laissez pas traîner des documents imprimés sur l'imprimante, surtout si cette dernière est installée dans des espaces accessibles au public (accueil, etc.).

WIR, DIE GEBÄUDETECHNIKER.

NOI, I TECNICI DELLA COSTRUZIONE.

NOUS, LES TECHNICIENS DU BÂTIMENT.

Renseignements :
Le responsable informatique de suissetec se tient à votre disposition pour tout autre renseignement.
Tel. 043 244 73 44
Fax 043 244 73 79

Note
L'association ISSS et suissetec ne pourra être tenue responsable des dommages éventuels occasionnés par l'utilisation, correcte ou erronée, du programme en 10 points.

Informations de source
Cette notice technique a été élaborée par ISSS (Information Security Society Switzerland), Bollwerk 21, CH-3001 Bern, Tel. +41 31 311 5300, http ://www.isss.ch

ISSS Information Security Society Switzerland

Notice technique «Sécurité informatique pour les PME», © suissetec, Janvier 2018

suissetec

Association suisse et liechtensteinoise de la technique du bâtiment
Auf der Mauer 11, Case postale, 8021 Zurich
T 043 244 73 00, F 043 244 73 79
www.suissetec.ch