

Mémento à l'attention des utilisateurs des systèmes d'information

Mairie de Signes

FUTURZO



Les réseaux du futur

UTILISATION DES SYSTEMES D'INFORMATION ACCES AUX DONNEES

L'utilisation à des fins privées de systèmes d'information non classifiés de défense est tolérée sous réserve qu'elle reste exceptionnelle et sans impact sur le bon fonctionnement général du système ou sur la bonne marche du service.

L'utilisation à des fins personnelles de systèmes d'information sensibles est interdite.

En utilisant les ressources informatiques de la mairie de Signes, l'utilisateur a pleinement conscience que même si, en principe, personne ne doit accéder à son espace personnel clairement indiqué :

- du personnel soumis à une obligation de non divulgation tels les administrateurs, auditeurs, contrôleurs et inspecteurs de la sécurité des systèmes d'information (SSI),
- les agents automatiques tels les anti-virus, des logiciels informatiques de contrôle de la conformité, etc. peuvent y être autorisés dans le cadre de leurs missions ou en cas d'anomalie ou d'incident réel ou supposé menaçant la sécurité ou le fonctionnement des dites ressources.

(Charte RGPD – Mairie de Signes)

A défaut d'être clairement identifiés comme privés, les dossiers, fichiers et courriels sont présumés professionnels.

- 1) Y compris les logiciels dits « portables », c'est-à-dire n'ayant pas besoin d'être installés ;

2) Un mot de passe est considéré sûr s'il est d'une longueur minimale de 9 caractères et comporte au minimum des

majuscules, minuscules, chiffres, caractères spéciaux et accentués.

3) Clés USB, disques durs externes, CD-ROM, etc.

4) Comme par exemple les sites incitant à la haine raciale, au terrorisme, etc.

5) Comme par exemple des sites pornographiques, de jeu en ligne, etc.

REACTION AUX INCIDENTS

L'utilisateur **doit rendre compte de tout incident** (réception de courriel suspect, détection virale, perte ou vol de support, doute...) et prendre les mesures conservatoires prescrites à son niveau.

Réaction de l'utilisateur en cas d'alerte virale :

- Interrompre toute activité sur la machine suspecte.
- **Ne pas arrêter ni redémarrer** la station.
- Débrancher le câble réseau (voir photo).
- Prévenir l'administrateur Réseaux de la mairie.
- Lui fournir tous les renseignements utiles et suivre ses directives.
- Tenir à sa disposition tous les supports amovibles ayant été connectés à la station.
- Si le poste est multi-utilisateurs (station Internet, autre..), verrouiller la station et placer une affichette interdisant l'utilisation du poste.



Administrateur Réseaux :
Jacques ACHARD

04 94 02 12 78

STATION DE TRAVAIL

Respect des configurations :

Il est interdit de modifier ou de tenter de modifier son environnement de travail logiciel ou matériel (ajout et suppression de programmes, de supports externes ou de périphériques, modification de paramétrage...) sans autorisation. Sont en particulier interdits :

- l'utilisation de logiciels¹/fichiers dont le droit de licence n'a pas été acquitté ou d'origine douteuse ;
- les logiciels de jeux ;
- les utilitaires (audio, vidéo, écran de veille, etc.) autres que ceux agréés par la mairie de Signes ;
- l'utilisateur contrôle que l'antivirus installé sur sa station est présent et mis à jour récemment.

Utilisation de moyens personnels :

La connexion **d'équipements et supports amovibles privés** sur un système de la mairie de Signes est **interdite**.

Autorisation d'accès :

- L'utilisateur doit verrouiller sa session (CTRL+ALT+SUPPR) lorsqu'il s'absente ;
- L'utilisateur doit choisir un mot de passe sûr² et le changer régulièrement conformément aux préconisations en vigueur sur le système auquel il se connecte ;
- Les droits d'accès et privilèges sont personnels et ne doivent pas être cédés : l'utilisateur ne divulgue pas et ne laisse pas son mot de passe facilement accessible.

Protection de l'information :

Il faut respecter les règles de protection de l'information et des systèmes qui les supportent, en

fonction de leur niveau de protection ou de confidentialité ;

- il est interdit de connecter des supports³ classifiés sur un système de protection faible ;
- le marquage de la protection ou classification des fichiers et courriels doit être effective ;
- si nécessaire, les informations doivent être chiffrées avec des moyens adéquats (le logiciel VERACRYPT permet de chiffrer des informations sensibles)

MESSAGERIE

Une messagerie réputée professionnelle :

A défaut d'être clairement identifié comme privé (idéalement dans son objet), un courriel émis à partir d'une station de travail mise à disposition par l'administration est présumé avoir un caractère professionnel de sorte que l'administration peut, en cas de besoin, accéder à son contenu.

Protection de l'information :

Un message envoyé sur un réseau échappe au contrôle de son expéditeur : il peut être redistribué à d'autres destinataires que ceux initialement visés. En particulier :

- l'utilisateur doit être vigilant lors de l'utilisation des fonctionnalités « transférer » et « répondre à tous » de la messagerie ;
- l'envoi d'information sensible en clair sur Internet est interdite. Les documents à transmettre doivent préalablement avoir été chiffrés (à l'aide du logiciel VERACRYPT pour les informations sensibles non classifiées). VERACRYPT permet de chiffrer des documents sensibles non classifiés.

INTERNET

Sont consultés des sites dont le contenu ne contrevient pas à la loi⁴ et sans conséquence pour la sécurité ou la réputation de la mairie de Signes. L'accès à certains sites web peut être bloqué pour répondre à des impératifs de sécurité ou au motif d'un contenu jugé offensant ou inapproprié⁵.

Utilisez les médias sociaux avec prudence, en préservant secret et neutralité !

SUPPORTS AMOVIBLES

Les supports amovibles de la mairie de Signes³ sont toujours placés sous la responsabilité et la surveillance du détenteur du support, notamment en cas de perte ou de vol. Leur nombre doit être limité au strict nécessaire.

Tout support amovible modifié hors du réseau auquel il va être connecté doit **obligatoirement** subir un contrôle antiviral sur une station blanche.

En cas de détection virale, le support amovible source de l'alerte peut être placé sous séquestre par un agent de SSI :

- à des fins d'investigation sur demande de l'administrateur Réseaux ;
- afin de s'assurer que la totalité de la menace a bien été traitée.

Il est recommandé de vider régulièrement ses clés USB et de n'y conserver que les fichiers nécessaires. Cela permet de minimiser les conséquences d'une perte ou d'un vol, les supports amovibles ne devant pas être utilisés comme un moyen de sauvegarde.

Sauf exception dûment autorisée par un agent de SSI, seul un support enrôlé est autorisé, après contrôle antiviral, à être connecté sur un poste de la force d'action navale.