Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Sécurité des Postes de Travail

Carte Acteurs de l'Administration de l'Etat
Carte Acteurs des Collectivités Territoriales

Les 9 mesures énoncées dans le présent document, permettent de vous prémunir contre les risques courants qui peuvent affecter le poste de travail utilisé pour les demandes de Cartes Agents. Elles ne prétendent pas avoir un caractère d'exhaustivité. Elles représentent cependant le socle minimum des règles à respecter pour protéger les informations que vous allez manipuler.

Ces recommandations sont en partie issues des référentiels de bonnes pratiques de sécurité publiés par l'Agence Nationale de la Sécurité des Système d'Information (ANSSI)[1]. Ne pas les suivre vous expose à des risques d'incidents majeurs[2].

Chaque mesure décrite ci-dessous est complétée par un ou plusieurs points de contrôle. Ces points de contrôle simples et pragmatiques doivent vous permettre de déterminer si vous appliquez actuellement la mesure ou non. La première partie du document présente les règles propres au poste de travail et à sa configuration. La seconde partie se concentre sur les bonnes pratiques d'utilisation de ce poste de travail.

Dans la suite du document, le terme « poste de travail » désigne le poste informatique utilisé pour la commande et la gestion des Cartes Agents délivrées pour la collectivité territoriale. Un « administrateur » désigne la personne qui dispose des droits suffisants pour configurer/administrer le poste de travail.

ANTS - v.1.1
09/11/2012

---

[1] *Guide d'hygiène informatique* : http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
Portail de la sécurité informatique : http://www.securite-informatique.gouv.fr/

[2] En vertu des articles 323-1 à 323-7 du Code pénal applicable lorsqu'une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc. Les peines encourues varient de 1 à 3 ans d'emprisonnement assortis d'une amende allant de 15.000 à 225.000 euros pour les personnes morales.

1 Sécurité relative à l'utilisation du poste de travail

Mesure 1 - Chaque personne ayant accès au système doit être connue

Chaque personne ayant accès au poste de travail doit utiliser une session de travail nominative et personnelle, protégée par un identifiant (nominatif) et un mot de passe. Les sessions partagées ou communes sont donc à proscrire. Une liste des personnes ayant accès (ou ayant eu accès) au poste de travail doit être conservée par le responsable de la collectivité territoriale.

- ☐ **Chaque utilisateur dispose de sa session de travail personnelle (identifiant/mot de passe)**
- ☐ **La liste des utilisateurs du poste de travail existe et est tenue à jour**

Mesure 2 - Ne pas avoir les « droits d'administrateur » sur le poste

L'accès aux fonctions d'administration du poste de travail doit être restreint aux seuls administrateurs de celui-ci. Il doit donc y avoir un compte administrateur en plus du ou des comptes utilisateurs (mentionnés dans la mesure 1). Les applications nécessitant des droits de niveau « administrateur » pour leur exécution doivent, dans la mesure du possible, être évitées et l'installation et la mise à jour de logiciels sur le poste de travail sont sous le contrôle de l'administrateur du poste de travail. L'utilisation d'internet à partir d'une session administrateur est à proscrire.

- ☐ **Les utilisateurs du poste de travail ne disposent pas des droits « administrateur »**
- ☐ **L'administrateur n'utilise pas (ou peu) sa session pour aller sur Internet**

Mesure 3 - Le poste de travail est protégé contre les virus.

Un unique logiciel antivirus doit être installé (par l'administrateur) sur le poste de travail et configuré pour recevoir ses mises à jour automatiquement. L'utilisateur du poste de travail ne doit pas pouvoir le désactiver.

- ☐ **Un unique antivirus est installé et configuré sur le poste de travail**
- ☐ **Un utilisateur quelconque du poste de travail ne doit pas pouvoir le désactiver**

Mesure 4 - Le poste de travail exploite des logiciels « à jour »

L'administrateur doit régulièrement procéder à la mise à jour du système d'exploitation et des logiciels installés sur le poste de travail (notamment du navigateur web). Ces mises à jour permettent de contrer les dernières failles de sécurité. Les mises à jour critiques des systèmes d'exploitation peuvent être installées sans délai en programmant une vérification automatique périodique hebdomadaire.

- ☐ **La mise à jour du système d'exploitation est programmée de façon automatique**
- ☐ **L'état du poste de travail est régulièrement contrôlé par l'administrateur**

Mesure 5 - Le poste de travail est protégé un pare-feu (firewall)

Un unique pare-feu logiciel (compatible avec l'antivirus installé sur le poste de travail) ou matériel doit protéger le poste de travail. Les systèmes d'exploitation Windows XP et Windows 7 sont déjà équipés d'un pare-feu compatible avec les antivirus actuels.

- [ ] **Un unique pare-feu (matériel ou logiciel) protège le poste de travail**

Mesure 6 - L'exécution automatique des clés USB doit être désactivée.

Les supports amovibles (clés USB, disques durs externes, téléphones portables, baladeurs numériques, …) sont un moyen privilégié de propagation des codes malveillants et de fuite de données. L'administrateur du poste de travail doit donc interdire techniquement la connexion de ces supports amovibles sauf si c'est strictement nécessaire. Dans le cas contraire, l'exécution automatique (autoruns) depuis de tels supports doit être désactivée.

- [ ] **Les supports amovibles de stockage ne peuvent être connectés sur le poste de travail**

Mesure 7 - Limiter l'utilisation des technologies sans-fil

Les technologies sans fil (WiFi, Bluetooth, 3G) présentent de nombreuses failles de sécurité si elles sont mal configurées. L'usage de ces technologies doit être évité, au profit d'une connectivité filaire standard. Lorsque les technologies sans fil sont utilisées, les connexions doivent être sécurisées.

- [ ] **Le poste de travail est connecté au réseau à l'aide d'un câble réseau standard**
- [ ] **Le clavier et la souris du poste de travail sont connectés à l'aide de fils**

2 Sécurité relative à l'environnement de travail

Mesure 8 - Travailler sur un bureau dégagé

L'espace de travail ne doit pas être encombré par du matériel inutile dans la fonction du poste et aucun matériel suspect ne doit être branché sur le poste. En cas de doute, demandez conseil à l'administrateur du poste de travail. Aucune information confidentielle (code PIN, mot de passe) ne doit être apparente sur l'espace de travail. De la même façon, aucune Carte Agent active ne doit être laissée à la portée d'une tierce personne.

- ☐ **Le bureau du poste de travail est dégagé (pas de matériel inconnu à proximité)**
- ☐ **Les Carte Agents ne sont pas stockées à proximité du poste de travail**
- ☐ **Aucun élément sensible (mot de passe, code PIN) n'est affiché sur le poste de travail**

Mesure 9 - Soyez prudents

- Ne jamais ouvrir les pièces jointes d'un email ou cliquer sur des liens sans vous assurer de la fiabilité du message en termes de source d'émission et de contenu.
- Ne « surfez » pas sur des sites illégaux ou potentiellement vecteurs de risques lorsque vous êtes sur le poste de travail
- Refusez toujours les installations de logiciels qui vous sont proposées spontanément lorsque vous surfez sur Internet et refusez systématiquement l'installation des barres d'outils (« *toolbar* ») à destination des navigateurs internet.
- N'installez jamais des programmes piratés et/ou qui ne sont pas nécessaires à l'utilisation du poste de travail.

- ☐ **Les consignes ci-dessus ont été diffusées aux utilisateurs du poste de travail**
- ☐ **Les navigateurs installés n'ont pas de barres d'outils spécifiques (Ask, Google, Hotmail, …)**
- ☐ **Les logiciels installés sur le poste de travail proviennent d'éditeurs fiables**