

Synthèse des bonnes pratiques de l'utilisateur du Système d'Information

Les principes

Ces bonnes pratiques s'appliquent à tous :

- les utilisateurs, quelle que soit leur localisation,
- les postes de travail, fixes, portables, PDA...,
- les supports informatiques de données (clés USB, disques externes, CD, DVD, ...).

Organisation

- Le poste de travail est confié à une personne nommément désignée qui doit veiller à :
 - la protection physique de la ressource matérielle et logicielle qui lui est confiée,
 - la conformité du poste (logiciels, configuration, ...).
- Cette vigilance s'exerce aussi bien sur le lieu de travail qu'à l'extérieur (train, hôtel, domicile, ...).
- Les demandes d'attribution des droits aux personnes (accès aux systèmes, réseaux, applications) sont formulées par la hiérarchie.
- Les demandes éventuelles de dérogation aux règles doivent être argumentées, et validées par la hiérarchie et la chaîne fonctionnelle de la Sécurité des Systèmes d'Information :
Personne ressource en informatique - Responsable de l'équipe informatique de centre -
Responsable de la sécurité des systèmes d'information (RSSI)

Les textes de référence

- Les bonnes pratiques de ce mémento sont consécutives aux textes suivants, consultables sur le site intranet www.inra.fr/ssi :
- Politique de sécurité des systèmes d'information de l'Inra,
- Charte utilisateur pour l'usage des ressources informatiques de l'Inra,
- Charte des administrateurs de ressources informatiques de l'Inra,
- Procédures de contrôle relatives à l'utilisation des ressources informatiques de l'Inra,
- Règlements des unités et des centres Inra,
- Supports pédagogiques de sensibilisation SSI,
- Règlementation officielle (Code civil, Code pénal, Code du travail, ...).

La responsabilité de l'utilisateur

L'utilisateur engage sa responsabilité à respecter les lois, les règles et les bonnes pratiques.

- Lors de la création d'information, l'utilisateur doit en évaluer sa sensibilité.
- La sensibilité d'une information est définie par l'impact (opérationnel, financier, juridique, social, d'image...) d'une perte de disponibilité, d'intégrité, de confidentialité ou de preuve.
- Lorsqu'un utilisateur gère des données sensibles, il doit en informer la hiérarchie et la fonction SSI afin que les protections adaptées soient mises en place.

Installation et contrôle d'accès

Configuration des équipements

- Chaque utilisateur doit respecter les configurations standard des équipements, spécifiées par l'unité ou par le centre.
- Il lui est interdit d'y faire toute adjonction, matérielle ou logicielle, sans l'accord de sa hiérarchie.
- L'utilisation de logiciels sans licences officiellement et régulièrement acquises est interdite.

Contrôle d'accès : les principes

- L'accès au poste de travail est assujéti à un contrôle d'authentification individualisé (identifiant et mot de passe, carte à puce, ...).
- L'utilisateur doit verrouiller sa session dès qu'il quitte son poste de travail.
- L'accès aux réseaux, serveurs et applications nécessite un identifiant authentifié personnel et inaccessibles.
- Un ordinateur portable fourni par l'Inra est destiné à une utilisation professionnelle. Il ne doit pas être utilisé par des personnes qui ne sont pas rattachées à l'Inra, les membres de la famille par exemple.

Contrôle d'accès : l'authentification

- Le mot de passe ne définit pas un droit ; il a pour objectif d'authentifier une identité afin de pouvoir engager la responsabilité de l'utilisateur.
- Le mot de passe compte au moins 8 caractères.
- Il doit être composé d'une combinaison de caractères alphabétiques (majuscules et minuscules), chiffres et caractères spéciaux.
- Il ne doit pas utiliser de termes repérables (nom propre, identifiant, prénom, mot du dictionnaire, ...).
- Il ne doit en aucun cas être divulgué à une autre personne.
- Il ne doit pas être noté. Si une trace écrite est nécessaire, elle doit être protégée comme une information confidentielle.

Propriété Intellectuelle

Logiciels et développements

- L'installation d'un logiciel doit être faite dans le respect de la réglementation ; l'installation d'un logiciel sans licence légale et professionnelle est strictement interdite.
- En cas de doute, consulter le RSSI (Responsable de la Sécurité des Systèmes d'Information).
- Sauf clause contractuelle explicite, tout logiciel développé pour l'Inra est la propriété intellectuelle de l'Inra.

Informatique et libertés

Données à caractère personnel

- L'utilisateur s'engage à respecter les obligations légales liées à la protection des données à caractère personnel : confidentialité, respect de la finalité du traitement, suppression à la fin du traitement.
- Tout traitement comportant des données à caractère personnel est soumis à des formalités déclaratives préalables auprès de la CNIL ainsi qu'à des conditions de mise en œuvre.
- Contact : cmil@inra.fr

Protection du poste de travail

Protection logique

- Tout poste de travail doit être équipé d'un antivirus actif à jour. La neutralisation de l'antivirus est strictement interdite.
- Il est nécessaire d'effectuer un contrôle systématique de tous les supports externes utilisés (clés USB, CD, DVD, ...).
- Les utilisateurs nomades doivent se connecter régulièrement pour mettre à jour l'antivirus.

Protection physique

- Tout utilisateur d'un équipement doit utiliser les moyens de protection mis à sa disposition pour éviter le vol du matériel.
- La responsabilité de l'utilisateur pour la protection des informations et des biens s'exerce aussi à l'extérieur de l'Inra.
- En dehors des heures de travail, ranger les ordinateurs portables dans un meuble fermé à clé.
- Dans les lieux publics et les moyens de transport, rester vigilant sur ses matériels informatiques.

Échanges et communication

Messagerie

- Ne pas oublier que l'adresse de messagerie d'origine peut être usurpée.
- Analyser les caractéristiques du message ; s'il est atypique ne pas l'ouvrir.
- Ne pas transférer des messages à des personnes non habilitées à en connaître le contenu.
- Le nombre des destinataires en copie doit être mesuré.
- Ne pas cliquer sur des liens non professionnels dans les messages.
- Ne jamais accepter de déchiffrer ou de décompresser une pièce jointe si le mot de passe est transmis par la messagerie électronique.
- Les messages dont l'objet n'est pas spécifié « personnel » sont considérés comme professionnels, et peuvent être consultés par la hiérarchie.
- L'utilisation non professionnelle de la messagerie doit être modérée, loyale, non lucrative, conforme aux règles Inra, (notamment au devoir de réserve) et aux lois.
- Ne pas ouvrir de pièces jointes de messages non professionnels non sollicités.

Internet

- Les navigateurs Web donnent des informations sur la sécurité. En cas de doute, consulter le correspondant de sécurité.
- L'utilisateur détermine la confiance qu'il accorde au site en vérifiant le certificat.
- Lorsqu'un site est accédé avec le protocole https (indiqué dans la barre d'adresse), la connexion est chiffrée.
- Ne jamais enregistrer son mot de passe sur son poste.
- Le téléchargement d'œuvres protégées, sans avoir acquis les droits, est interdit par la loi.
- Limiter l'accès aux serveurs non professionnels à une utilisation raisonnable, non lucrative, loyale et conforme aux lois et aux règles Inra.
- Garder un regard critique sur la véracité des informations récupérées sur Internet.
- Ne pas oublier les devoirs de réserve, discrétion et confidentialité qui incombent à tout utilisateur.

Archivage, sauvegarde et stockage

Définitions

- **Archivage** = enregistrement des données sur un support de stockage afin de les conserver dans un état déterminé.
- **Sauvegarde** = duplication et mise en sécurité des données contenues dans un système informatique afin de pouvoir les restaurer en cas d'accident.

Archivage

- Les supports informatiques à conserver pour des raisons légales, contractuelles ou nécessaires à l'activité de l'Inra doivent faire l'objet de procédures d'archivage, tenant compte de la sensibilité des documents et des différents types de supports utilisés.

Sauvegarde

- La responsabilité des sauvegardes des données stockées localement incombe au détenteur du poste de travail sur lequel ces données sont stockées.
- Les fichiers confidentiels doivent être chiffrés sur leur support.

Stockage

- Le stockage des fichiers de travail courants sur un serveur est recommandé. Lorsque cela n'est pas possible, il est nécessaire d'effectuer des sauvegardes régulières et de stocker ces sauvegardes dans un local différent de celui du poste de travail.
- Conformément à la Charte utilisateur, la conservation de données personnelles sur le poste de travail est autorisée, à condition que cette utilisation soit modérée, loyale, non lucrative, conforme aux lois et aux règles Inra. Ces données doivent être placées dans un répertoire nommé « personnel ».
- Il est strictement interdit de chiffrer ces données privées personnelles sans l'autorisation de la Sécurité des Systèmes d'Information.

Départ de l'utilisateur

Lorsqu'un utilisateur cesse son activité dans une unité,

- Il doit transmettre à son directeur d'unité toutes les informations professionnelles qu'il gère, qu'elles soient stockées sur son poste de travail, sur des serveurs, ou sur des supports externes.
- Si son poste a été utilisé pour stocker des données confidentielles, il doit le signaler à la chaîne fonctionnelle de la Sécurité des Systèmes d'Information.
- Il doit restituer son poste de travail Inra, après avoir effacé toutes les données utilisées à des fins personnelles.
- Il doit garder à l'esprit que le devoir de discrétion et de confidentialité perdure à la fin du contrat.

Surveillance et Contrôle

La surveillance et le contrôle sont toujours effectués dans le respect des lois, des droits et devoirs associés (notamment ces contrôles sont toujours proportionnels au but recherché, c'est-à-dire la sécurité de l'Inra).

L'utilisateur est toujours informé au préalable de ces contrôles.