REPUBLIQUE FRANCAISE

INSTITUT NATIONAL DE LA RECHERCHE AGRONOMIQUE
147, Rue de l'Université – 75338 PARIS CEDEX 07
Tél. : 01 42 75 90 00

DIRECTION DU SYSTÈME D'INFORMATION **Note de service N° 2008-51**
du 13 juin 2008

OBJET : CHARTE UTILISATEUR POUR L'USAGE DES RESSOURCES INFORMATIQUES DE L'INRA

Modifie la note de service n° 2005-22 du 8 avril 2005
DIFFUSION TOTALE

Résumé

Les systèmes d'information, notamment ceux qui sont mis en œuvre par des moyens informatiques, ont pris une importance grandissante au cœur des processus d'animation scientifique, de gestion et de gouvernance de l'ensemble de nos activités.

Face aux menaces qui pèsent sur nos systèmes d'information, l'Institut se doit d'exiger, de ses agents comme de ses outils collectifs, dans son fonctionnement interne comme dans ses relations partenariales, une protection professionnelle et rigoureuse des informations et des services de traitement et de transport de l'information.

Dans ce cadre, l'Inra adopte une « Charte utilisateur pour l'usage des ressources informatiques de l'Inra » et différents textes précisant les droits et obligations de l'Inra et des usagers de ses ressources informatiques dans le cadre de leurs activités professionnelles.

Cette « Charte utilisateur pour l'usage des ressources informatiques de l'Inra » a pour objectifs de définir les conditions d'utilisation et les règles de bon usage des ressources informatiques de l'Inra.

Elle vise en tout premier lieu à définir les conditions d'un juste équilibre dans les rapports entre employeurs et agents publics, équilibre indispensable à la pérennité de nos processus de travail.

Loyauté, transparence, sécurisation des ressources informatiques et des pratiques, aménagement du droit à l'utilisation à des fins personnelles sont les principes fondateurs qui en ont inspiré la conception.

Cette charte est complétée par les règlements suivants :
- Charte des administrateurs de ressources informatiques de l'Inra
- Procédures de contrôle relatives à l'utilisation des ressources informatiques de l'Inra

Charte utilisateur pour l'usage
des ressources informatiques de l'Inra

Notre Institut se propose d'adopter une « Charte utilisateur pour l'usage des ressources informatiques de l'Inra ».

Cette charte a pour première ambition de trouver un « juste équilibre » dans les rapports entre employeurs et agents public, afin de pérenniser et développer harmonieusement nos processus de travail, de plus en plus collaboratifs et informatisés.

En s'appuyant sur les travaux et recommandations de la CNIL - Commission Nationale de l'Informatique et des Libertés, l'Inra souhaite ainsi privilégier l'autorégulation pondérée, l'autoresponsabilisation, l'engagement de l'agent public à une certaine autodiscipline, tout en privilégiant le dialogue avec les instances de co-régulation que sont le Comité Technique Paritaire, les Conseils de gestion des centres et les Conseils d'unités.

Notre volonté de mise en avant de la discussion et de l'appropriation collectives est renforcée par des principes de transparence, d'information et de proportionnalité afin que le « juste équilibre » entre sécurité et liberté d'utilisation des ressources informatiques puisse trouver une mise en œuvre optimale au sein de notre organisme.

1. Objet de la charte

La présente charte a pour objet de définir les conditions d'utilisation et les règles de bon usage des ressources informatiques de l'Inra.

Elle précise la responsabilité des utilisateurs, dans le respect de la législation en vigueur, afin de promouvoir un usage correct des ressources informatiques, avec des règles minimales de courtoisie et de respect d'autrui.

Ces règles découlent en grande partie de textes de référence, notamment le code pénal, le code de la propriété intellectuelle, les lois relatives « à l'informatique, aux fichiers et aux libertés », la charte déontologique du GIP Renater, appliqués dans le contexte particulier des droits et obligations des fonctionnaires Ces textes concernent en particulier :

- la disponibilité et l'intégrité des systèmes et des données ;
- la confidentialité des informations ;
- la falsification et la fraude informatiques ;
- l'illégalité des contenus (propagation d'idées racistes, xénophobes, …) ;
- les infractions liées à la propriété intellectuelle et aux droits connexes (copies illégales d'œuvres protégées, …).

La présente charte est applicable à l'ensemble des agents et des personnes autorisées à utiliser les ressources informatiques de l'Inra.

Le manquement aux règles édictées dans cette charte peut donner lieu à l'application de sanctions disciplinaires ou pénales en fonction de la nature et de la gravité des faits reprochés et de leurs conséquences sur le préjudice subi par l'Inra.

Cette charte est complétée par les règlements suivants :

- Charte des administrateurs de ressources informatiques de l'Inra ;
- Procédures de contrôle relatives à l'utilisation des ressources informatiques de l'Inra ;
- les règlements des centres Inra et des unités.

2. Principes généraux d'accès aux ressources informatiques

L'utilisation des ressources informatiques est destinée à l'activité professionnelle des utilisateurs, conformément à la législation en vigueur.

Toutefois une utilisation ponctuelle des ressources informatiques pour un motif personnel est autorisée, à la condition qu'elle reste dans des limites raisonnables.

Les ressources informatiques concernées par cette charte sont tous les équipements informatiques, réseaux, systèmes d'information administrés par l'Inra. Les équipements incluent notamment les serveurs, les postes de travail, les équipements d'acquisition, de stockage, de restitution et d'impression. Les réseaux incluent les infrastructures de communication, internes aux bâtiments, entre les bâtiments, entre les sites Inra, et avec l'Internet, les équipements de communication, ainsi que les services de communication associés. Les systèmes d'information incluent, entre autres, les systèmes d'information de recherche et de gestion, et les applications informatiques associées, les divers services de communication d'informations, tels que le Web, la messagerie, les forums. Ces listes ne sont pas limitatives.

On désignera par « utilisateur » toute personne qui utilise les ressources informatiques de l'Inra, à l'exception des simples visiteurs de services Internet.

Les activités professionnelles sont les activités de recherche, d'enseignement, de développement technique, de transfert de technologies, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentation de nouveaux services présentant un caractère d'innovation technique, ainsi que toute activité administrative, de gestion ou d'appui à la recherche découlant ou accompagnant ces activités. L'utilisation des ressources informatiques de l'Inra est autorisée pour les activités syndicales et sociales relevant de l'Inra.

L'utilisation des ressources informatiques de l'Inra, notamment l'ouverture d'un compte ou la connexion d'un équipement sur le réseau, est soumise à autorisation. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Ces autorisations peuvent être retirées à tout moment. Toute autorisation prend fin de plein

droit lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée. Les utilisateurs disposeront cependant d'un délai de deux mois avant la fermeture effective des autorisations d'accès, afin de terminer les opérations en cours et d'effectuer les sauvegardes nécessaires.

La connexion d'équipements informatiques mobiles, propriété de l'Inra ou personnels, aux réseaux de l'Inra est soumise à des règles particulières, concernant notamment leur protection contre les virus et les intrusions. Ces règles sont ou seront décrites dans un document dédié « Connexion de postes nomades ». Une attention particulière doit être apportée au respect des règles concernant les licences logicielles et la propriété intellectuelle.

2.1. Garanties accordées aux agents

L'Inra est conscient des risques d'atteinte aux libertés individuelles du fait des multiples procédures de collecte d'informations et donc de traitements automatisés des données personnelles qui peuvent en découler.

Dans ce cadre, et au regard des risques éventuels pour les individus, sont privilégiés :

- la discussion collective au niveau pertinent (Comité Technique Paritaire, Conseils de gestion des départements pour le niveau national, Conseils de gestion au niveau des centres, Conseils de service au niveau des unités) ;
- l'information préalable des agents ;
- le droit d'opposition dans le cadre du traitement de données nominatives ;
- le principe de proportionnalité : en ce sens ne peuvent pas être apportées aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas proportionnées au but recherché.

L'Inra respecte le principe de protection de l'intimité de la vie privée de l'agent public sur son lieu de travail et donc du secret des correspondances et des fichiers relevant des activités personnelles, syndicales ou sociales. Ces messages et ces fichiers doivent être placés par les utilisateurs dans des dossiers dont les noms sont explicites : personnel, syndical (ou le nom du syndicat), social (ou adas). Aucun autre utilisateur que le propriétaire n'est autorisé à accéder au contenu de ces dossiers.

2.2. Droits et Propriétés

Si tout message est, en principe, la propriété de son destinataire, les droits de propriété intellectuelle afférents au message en tant qu'œuvre appartiennent à l'émetteur qui en est donc responsable.
Toutes les données issues de l'activité professionnelle sont propriété de l'employeur. À ce titre elles sont couvertes par la loyauté, la confidentialité et le secret professionnel afférents au statut du fonctionnaire et/ou couverts par des clauses contractuelles.
Dans ce cadre, leurs utilisations doivent respecter des principes de prudence, de bonnes pratiques ainsi que des obligations contractuelles en vigueur.

2.3. Sécurisation des ressources informatiques

Les principes décrits dans cet article sont complétés par les documents d'administration des ressources informatiques.

L'utilisation des ressources informatiques par les utilisateurs est enregistrée pendant un an.

L'objectif de l'Inra est d'assurer la sécurité des systèmes d'informations, et non de réaliser un contrôle individuel de l'activité des agents. Les seules informations nominatives qui peuvent être conservées au-delà d'une année concernent les volumes de ressources utilisées. Les traces détaillées de l'utilisation des ressources informatiques par les utilisateurs peuvent être conservées, afin de permettre la détection d'intrusion ou de non respect des règles, au maximum un an.

Les espaces de stockage des postes de travail et des serveurs doivent être contrôlés par des antivirus.

Des processus automatiques analysent tous les espaces de stockage d'informations, y compris les espaces personnels, pour détecter la présence de codes exécutables, notamment la présence de virus informatiques, susceptibles de compromettre la sécurité de l'équipement qui héberge ces espaces de stockage ou celle de ressources externes à cet équipement. Les administrateurs de ressources collectives doivent mettre ces codes hors d'état de nuire.

Afin de renforcer la sécurité de ces ressources informatiques, l'Inra met en place des dispositifs de filtrage des communications informatiques.

Seuls certains protocoles Internet sont autorisés. Les règles de filtrage sont établies par le service responsable de l'administration des ressources informatiques de l'Inra, en fonction des besoins exprimés par les utilisateurs, et en tenant compte notamment des avis des équipes de sécurité du GIP RENATER et de la Direction centrale de la sécurité des systèmes d'information. Elles sont soumises pour approbation au Responsable de la sécurité des systèmes d'information.

Afin de limiter la réception de messages non sollicités et de messages contenant des virus, l'Inra met en place des dispositifs de filtrage des messages électroniques.

Ces dispositifs fonctionnent selon des règles fixées par les administrateurs de réseaux. Ils sont entièrement informatiques, et garantissent qu'aucune personne ne peut avoir connaissance du contenu des messages.

Les règles de filtrage des communications et des messages sont communiquées aux utilisateurs par les administrateurs des réseaux.

L'Inra, après les procédures de consultation appropriées, peut mettre en place des dispositifs de filtrage de sites non autorisés sur Internet. Toute mesure de filtrage fera l'objet de l'information des utilisateurs.

3. Règles d'utilisation, de sécurité et de bon usage des ressources informatiques, à respecter par les utilisateurs

L'Inra, en fonction de l'état de l'art et des coûts liés à la mise en œuvre, s'engage à prendre les mesures adaptées à un niveau de sécurité approprié au regard des risques évalués et de la valeur des ressources et des informations à protéger.

Chaque utilisateur est responsable de l'usage des ressources informatiques mises à sa disposition et s'engage à ne pas effectuer des opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement de ces ressources, sur l'intégrité des systèmes d'information, et sur les relations internes et externes de l'Institut.

Chaque utilisateur a la charge, à son niveau, de contribuer à la sécurité générale des systèmes d'information et à celle de l'Inra. L'utilisation des ressources informatiques doit être rationnelle, et conforme à l'intérêt du service, contribuant ainsi à éviter sa saturation ou son détournement.

Toute anomalie constatée, susceptible d'affecter la sécurité des ressources informatiques, doit être signalée à la Personne ressource informatique de l'unité ou à l'Équipe informatique de centre.

L'Inra ne pourra être tenu pour responsable des détériorations d'informations ou des manquements commis par un utilisateur qui ne se sera pas conformé à ces règles. Tout manquement à ces stipulations engage la responsabilité personnelle de l'utilisateur, qui en assume les entières conséquences.

3.1. Obligations à respecter par tout utilisateur

- Il doit assurer la protection de ses informations et il est responsable des droits qu'il donne aux autres utilisateurs, il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde, individuels ou collectifs, mis à sa disposition.
- Il doit choisir des mots de passe sûrs, gardés secrets, et en aucun cas ne doit les communiquer à des tiers.
- Lorsqu'il quitte un poste de travail, il doit verrouiller ou fermer les sessions ouvertes, afin de ne pas laisser des ressources ou des services disponibles sans identification.
- Il doit se conformer aux obligations de discrétion professionnelle, de réserve, et de bonne moralité afférentes au statut de fonctionnaire
- Il doit respecter l'ensemble des lois d'ordre pénal ou civil en vigueur, notamment celles relatives
    - aux publications à caractère raciste, pédophile, injurieux, diffamatoire,
    - au harcèlement sexuel ou moral,
    - à l'utilisation des logiciels,
    - au droit d'auteur.
- Il doit appliquer les consignes de sécurité complémentaires définies par le centre et par l'unité auxquels il appartient.
- Il doit suivre les règles en vigueur au sein de l'unité pour toute installation de logiciel.

3.2. Interdictions à respecter par tout utilisateur

- Il ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues pour ce serveur ou sans y être autorisé par les responsables habilités.
- Il ne doit pas tenter de lire, modifier, déposer ou détruire des données sur un serveur autrement que par les dispositions prévues pour ce serveur ou sans y être autorisé par les responsables habilités.
- Il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède.
- Il ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers.
- Il ne doit pas connecter un matériel sur le réseau sans autorisation.
- Il ne doit pas mettre à la disposition de personnes non autorisées un accès aux ressources informatiques de l'Inra.
- Il ne doit pas, par quelque moyen que ce soit, proposer ou rendre accessible aux tiers des informations confidentielles ou contraires à la législation en vigueur.
- Il ne doit pas télécharger ou diffuser des données en violation des lois protégeant les droits d'auteur, quel que soit le domaine (écrits, images, logiciels, bases de données, …).
- Il ne doit pas contourner les restrictions d'utilisation d'un logiciel.

3.3. Utilisation et protection des ressources informatiques à des fins personnelles

L'utilisation des ressources informatiques de l'Inra pour motif personnel ne doit pas être susceptible d'amoindrir les conditions d'accès professionnel à ces ressources. Elle est autorisée dans la mesure où elle ne porte pas atteinte au bon fonctionnement du service, et ne met pas en cause la productivité de l'Institut

L'ensemble des règles de cette charte s'applique également pour ce type d'utilisation.

Le devoir de réserve incombant à tout fonctionnaire doit être respecté.

La messagerie électronique peut également être utilisée pour un usage personnel, dans les limites imposées par le bon fonctionnement du service.

Conformément aux principes de droit, il est considéré qu'un message envoyé ou reçu depuis un poste de travail mis à la disposition de l'utilisateur par l'Inra revêt un caractère professionnel, sauf indication manifeste dans le sujet du message.

4. Modalités d'application

La présente charte s'applique à l'ensemble des personnes, personnels ou non de l'Inra, tous statuts confondus, autorisées à utiliser les ressources informatiques de l'Inra.

Lorsqu'un compte est ouvert pour un utilisateur, celui-ci doit déclarer avoir pris connaissance de la présente charte et des documents associés, et s'engager à les respecter. Cette déclaration sera effectuée par la procédure en vigueur au moment de l'ouverture du compte, procédure qui peut être notamment la signature d'un document ou l'exécution d'une application informatique.

Chaque Directeur d'unité est chargé de faire respecter cette charte.

La présente charte est publiée sur l'intranet Inra : https://intranet.inra.fr/ssi/reglements/charte

Elle sera complétée par des guides de procédures relatives aux types d'utilisation et d'administration des ressources informatiques.

Elle sera réactualisée régulièrement afin de tenir compte du contexte juridique et technologique en rapide évolution en matière de technologies de l'information.

Pour obtenir des informations complémentaires ou pour signaler des problèmes de sécurité, les utilisateurs peuvent s'adresser à la Personne ressource informatique de l'unité et l'Équipe Informatique de Centre.

Fait à Paris, le 13 juin 2008

La Présidente
de l'Institut National de la Recherche Agronomique

Glossaire

Compte : association d'un utilisateur, d'un identifiant (nom de « login ») et d'un droit d'accès à une ou plusieurs ressources informatiques. À un compte est associée une méthode d'authentification, par exemple un mot de passe, un certificat électronique, une carte à puce…

Administrateurs de systèmes et de réseaux : ils sont techniquement responsables du bon fonctionnement des ressources informatiques ; ce rôle est notamment dévolu aux équipes informatiques de centres.

RSSI : Responsable de la Sécurité des Systèmes d'Information. Il élabore la politique de sécurité, la propose à la Direction générale, contrôle son application et l'évalue.

PRI : Personne Ressource en Informatique. Il s'agit d'un rôle d'administration et d'assistance sur le matériel informatique et le logiciel, au niveau des unités.

Position dans le référentiel de la sécurité des systèmes d'information