Charte régissant l'usage du système d'information de l'Institut Agro Rennes-Angers

INTRODUCTION

L'Ecole nationale supérieure des sciences agronomiques, agroalimentaires, horticoles et du paysage (Institut Agro Rennes-Anngers) met en oeuvre un système d'information et de communication nécessaire à l'exercice de ses missions de service public. Il met ainsi à disposition de ses collaborateurs des outils informatiques et de communication.

La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication de l'Institut Agro Rennes-Angers. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d 'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de l'Institut Agro Rennes-Angers.

En raison de l'adhésion de l'Institut Agro Rennes-Angers au réseau RENATER, le signataire de la présente charte reconnaît également avoir pris connaissance de la charte déontologique RENATER – ci-après annexée – et en approuver les termes.

PROTECTION DES DONNEES A CARACTERE PERSONNEL

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ainsi que le règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données définissent les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elles ouvrent aux personnes concernées par les traitements un droit de demander l'accès à ses données personnelles, de demander la rectification, la limitation ou l'effacement de celles-ci ou encore de s'opposer au traitement.

L'Institut Agro Rennes-Angers a désigné un délégué à la protection des données (DPD). Ce dernier a pour mission d'informer et de conseiller l'établissement sur les obligations qui lui incombent de par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Il doit être consulté par le responsable des traitements de données à caractère personnel préalablement à leurs créations, leurs modifications ou leurs suppressions.

Il recense, dans un registre des traitements, la liste de l'ensemble des traitements de données à caractère personnel de l'Institut Agro Rennes-Angers qui sont portés à sa connaissance lors de leurs créations et au fur et à mesure de leurs mises en œuvre.

Cette liste est tenue à disposition de toute personne en faisant la demande.

Aux fins d'obtenir cette liste et/ou en cas de difficultés rencontrées lors de l'exercice de leurs droits, les personnes concernées peuvent saisir le délégué à la protection des données (DPD) à l'adresse dpd@agrocampus-ouest.fr qui se chargera de vous répondre sur la possibilité de faire droit à cette demande.

LE CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à tout utilisateur du Système d'Information et de communication de l'Institut Agro Rennes-Angers. L'utilisation à titre privé de ces outils est tolérée, mais doit être raisonnable et ne pas perturber le bon fonctionnement du service.

La charte est diffusée à l'ensemble des utilisateurs par note de service et, à ce titre, mise à disposition sur l'intranet (http://) de l'Institut Agro Rennes-Angers. Elle est systématiquement remise à tout nouvel arrivant.

Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques recommandées.

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre l'Institut Agro Rennes-Angers et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

QUELQUES DEFINITIONS

« **Utilisateur » :** toute personne autorisée à accéder au système d'information : agents titulaires et contractuels, étudiants, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels....

« **Chef de service** » : autorité hiérarchique directe

« **Système d'information** » : tous les équipements informatiques et de télécommunications ainsi que toutes les données qui y sont stockées.

« Identifiant » : code unique attribué à un utilisateur.

« Réseau » : ensemble des moyens techniques permettant la transmission des informations (moyens filaires et hertziens pour les données et pour la voix.)

« Sécurité » : tout ce qui concerne la protection du système d'information en terme d'intégrité, de confidentialité et de disponibilité.

« Equipements nomades » : moyens techniques mobiles susceptibles de stocker de l'information (ordinateurs portables, imprimantes portables, téléphones mobiles, « smartphones », CDROM, clés USB,…

« DSI » : Direction des systèmes d'information.

« PRI » : Personne ressource informatique, agent de l'école qui effectue dans le cadre de ses obligations de service et en marge de ses missions principales, une mission complémentaire d'appui à la DSI et sous sa direction.

« Personne responsable des traitements » : au vu du point 7 de l'article 4 du règlement (UE) 2016/679 du 27 avril 2016 et des dispositions de l'article 3 de la loi n°78-17 dite « Informatique et Libertés », « le responsable d'un traitement (…) est (…) la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens » (du traitement).

Concernant les traitements informatiques mis en œuvre dans l'école, il s'agit en principe du directeur.

I. REGLES D'UTILISATION DU SYSTEME D'INFORMATION DE L'INSTITUT AGRO RENNES-ANGERS

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité dans les conditions définies par l'école.

1 L'authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte ("login" ou identifiant) fourni à l'utilisateur lors de son arrivée dans l'école. Un mot de passe est associé à cet identifiant de connexion.

Les moyens d'authentification sont personnels et confidentiels.

Les recommandations suivantes sont adressées aux utilisateurs : Le mot de passe doit être composé de 7 caractères minimum combinant chiffres, lettres et caractères spéciaux. Il ne doit comporter ni le nom, ni le prénom ni l'identifiant d'ouverture de la session de travail. Il doit être renouvelé régulièrement.

2 Les règles de sécurité générales

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler à la DSI toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.
- Ne jamais confier son identifiant/mot de passe.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas copier, modifier, détruire les logiciels propriétés de l'école.
- Verrouiller l'accès à son ordinateur dès qu'il quitte son poste de travail (c'est-à-dire se mettre en mode demande du mot de passe).
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Ne pas connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par la DSI.
- Ne pas nuire au fonctionnement des outils informatiques et de communications.
- Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique et doit respecter les règles définies par l'école.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information de l'école sans l'accord préalable de la DSI.

II. LES MOYENS INFORMATIQUES

1 Configuration du poste de travail

L'utilisateur d'un poste de travail, individuel ou collectif, doté des outils informatiques nécessaires à l'accomplissement de ses missions, et mis à disposition par l'école ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage principal notamment de connectivité réseau et de sécurité, ainsi que leur configuration physique ou logicielle[1].
- Déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement nomade »)

La durée de la mise à disposition, longue ou courte durée, ne modifie pas les engagements de l'utilisateur.

2 Equipements nomades.

On entend par « **équipements nomades** » tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB etc.. ..).
Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par chiffrement.

Quand un ordinateur portable se trouve dans le bureau de l'agent qui en a l'usage, cet ordinateur est réputé sous sa garde. Il doit en conséquence, prendre toutes les mesures adaptées à en prévenir le vol ou la détérioration.

L'utilisation de smartphones pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

3 Internet

Les utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient.
Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, l'ordre public, et ne met pas en cause l'intérêt et la réputation de l'institution, est admise.

[1] L'installation de logiciel par l'utilisateur sans l'avis de la DSI n'engage que la responsabilité de l'utilisateur. L'installation de certains logiciels (Cf liste adresse ENT) requiert impérativement un accord express de la DSI. Passer outre constitue un manquement caractérisé à la présente charte.

4 Messagerie électronique

1. Conditions d'utilisation

La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail de l'agent ni la sécurité du réseau informatique de l'école.

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

L'école s'interdit d'accéder aux dossiers et aux messages identifiés comme «personnel ».

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par et validées par la DSI :

- volumétrie globale de la messagerie,
- taille maximale de l'envoi et de la réception d'un message,
- nombre limité de destinataires simultanés lors de l'envoi d'un message,
- gestion de l'archivage de la messagerie.

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes.

Les utilisateurs peuvent consulter leur messagerie à distance, à l'aide d'un navigateur (webmail). Les fichiers qui seraient copiés sur un ordinateur extérieur utilisé par l'agent dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé.

2. Consultation de la messagerie

En cas d'absence d'un agent et afin de ne pas interrompre le fonctionnement du service, la DSI de l'école peut, ponctuellement transmettre au supérieur hiérarchique un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur (cf. conditions d'utilisation).

Le supérieur hiérarchique n'a pas accès aux autres messages de l'agent. L'agent concerné est informé dès que possible de la liste des messages qui ont été transférés. En cas d'absence prolongée d'un agent (longue maladie), le chef de service peut demander à la DSI, après accord du Directeurl, le transfert des messages reçus.

3. Courriel non sollicité

L'école dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter

leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

5 Espaces individuels de stockage de données

1. Conditions d'utilisation

Les espaces individuels de stockage de données mis à disposition des utilisateurs sont destinés à un usage professionnel. L'utilisation de ces espaces à des fins personnelles est tolérée si elle n'affecte pas le travail de l'agent ni la sécurité du réseau informatique de l'école.

Tout fichier qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée. A défaut, le fichier est présumé professionnel.

L'école s'interdit d'accéder aux fichiers identifiés comme «personnel».

Les fichiers qui seraient copiés sur un ordinateur extérieur utilisé par l'agent doivent être effacés dès que possible de l'ordinateur utilisé.

2. Accès de tiers aux espaces de stockage individuels

En dehors des cas où l'utilisateur a lui-même autorisé expressément un tiers à accéder à son espace de stockage individuel cet accès lui est strictement réservé sauf dans le cas précis où l'utilisateur est absent et non joignable et que la bonne marche du service exige d'accéder à des données stockées dans cet espace.

Sous cette double condition, seule la DSI est autorisé à accéder à cet espace et à transférer au chef de service de l'agent les données recherchées après avoir vérifiées la nature professionnelle de celles-ci. L'agent concerné est informé dès que possible de ce transfert.

III. TELEPHONE

L'école met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.
L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable. Des restrictions d'utilisation par les agents des téléphones fixes sont mises en place en tenant compte de leurs missions. A titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

L'école s'interdit de mettre en oeuvre un suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

L'école s'interdit d'accéder aux numéros complets appelés via l'autocommutateur mis en place et via les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, le service en charge de la téléphonie, sur demande du Directeur général, se réserve le droit d'accéder aux numéros complets des relevés individuels.

IV. UTILISATION DU SYSTEME D'INFORMATION PAR LES REPRESENTANTS DU PERSONNEL

Les représentants du personnel au Conseil de l'école et à la Formation Spécialisée de l'école utilisent, dans le cadre de leur mandat, les outils informatiques qui leur sont attribués pour l'exercice de leur activité professionnelle.

Cette utilisation pourra faire l'objet d'un protocole spécifique visant à concilier l'exercice du droit syndical et la neutralité du service public.

V. L'ADMINITRATION DU SYSTEME D'INFORMATION PAR LA DSI

La DSI assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de l'école. Elle s'appuie sur ses propres agents ainsi que sur les PRI.

Différents dispositifs techniques sont mis en place pour assurer cette mission et les agents de ce service disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Les personnels de la DSI, chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel.

Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur.

En revanche, ils doivent communiquer ces informations à leur hiérarchie si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité, ou si elles tombent dans le champ de l'article[2] 40 alinéa 2 du code de procédure pénale.

[2] Obligation faite à tout fonctionnaire d'informer sans délai le procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions.

1 Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information pour l'école et d'assurer la sécurité et la confidentialité des données sont mis en oeuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles.

2 Les systèmes automatiques de traçabilité

La DSI de l'écoe opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.

Elle s'appuie, pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent l'activité du système d'information et en particulier toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent notamment les données suivantes : dates, postes de travail, identifiant de l'utilisateur et objet de l'évènement.

La DSI est le seul utilisateur de ces informations.

3 Intervention sur le poste de travail

A des fins de maintenance informatique, la DSI peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur.

Par ailleurs en cas de besoin et notamment pour assurer la sécurité de l'ensemble du système d'information, la DSI peut être amenée à procéder à une intervention technique sur un poste informatique sans information préalable. Elle s'interdit alors d'accéder aux contenus stockés sur le poste.

4 Intervention sur les matériels connectés au réseau.

Tout matériel générant une perturbation sera isolé, le cas échéant déconnecté, du système d'information.

5 Intervention sur les données

Toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée ; le cas échéant supprimée.

VI. PROCEDURE APPLICABLE LORS DE L'ARRIVEE ET DU DEPART DE L'UTILISATEUR

1 Procédure d'arrivée

L'accès au système d'information est subordonné à l'inscription officielle de l'utilisateur dans l'annuaire de l'école. Cet enregistrement est réalisé par l'autorité concernée
selon le cas : Direction des formations et de la vie étudiante (DFVE) pour les étudiants, Direction des ressources humaines (DRH) pour toutes les autres personnes, quelque soit leur statut (agent titulaires et contractuels, stagiaires non étudiant, doctorants contractuel ou accueilli…)

L'autorisation, ouvrant droit à l'obtention d'un compte personnalisé avec mot de passe, n'est accordée qu'après acceptation de la présente Charte et le cas échéant des chartes INRA et RENATER. L'autorisation délivrée à l'utilisateur est strictement personnelle. Nul n'est autorisé à utiliser le compte d'autrui ou à prêter le sien. Chaque titulaire d'un compte est responsable de l'ensemble des actes effectués avec celui-ci.

2 Procédure de départ

Lors de son départ, l'utilisateur doit restituer à la DSI les matériels mis à sa disposition.

Concernant les données personnelles et identifiées comme telles : L'utilisateur veille à les effacer avant de quitter ses fonctions.

Concernant les données professionnelles : Il appartient au chef de service de l'utilisateur de s'assurer qu'il a accès aux données professionnelles nécessaire à la continuité du service et d'autoriser expressément, le cas échéant, toute copie totale ou partielle de ces données par l'utilisateur avant son départ. Cette autorisation est remise à l'utilisateur.

Les comptes et les données personnelles de l'utilisateur sont supprimés, dans un délai maximum de trois mois après son départ, sauf dérogation spéciale et expresse autorisée conjointement par l'utilisateur et par l'autorité qui a procédé à l'inscription de l'utilisateur dans l'annuaire de l'école (DFVE ou DRH).

VII. RESPONSABILITES- SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre.

Des sanctions en interne peuvent être prononcées, elles consistent :
- dans un premier temps, en un rappel à l'ordre et éventuellement à une restriction provisoire d'accès, émanant de la DSI, en cas de non-respect des règles énoncées par la présente charte ;
- dans un second temps, et en cas de renouvellement, après avis du Directeur général et du supérieur hiérarchique de l'agent, en l'engagement d'une procédure disciplinaire.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information est susceptible de sanctions pénales prévues par la loi.

VIII. ENTREE EN VIGUEUR DE LA CHARTE

La présente charte a été adoptée après information et consultation du comité technique.
Elle est applicable à compter de son adoption par le conseil d'administration.

ANNEXE : DISPOSITIONS LEGALES APPLICABLES

- Le règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée
- Dispositions Pénales :
  - Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain.
  - Dispositions pénales : art 323-1 à 323-7 du Code pénal.
  - Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels intégrée dans le code de la propriété intellectuelle
  - Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)
  - Loi n°2016-1321 du 7 octobre 2016 pour une République numérique
  - Code Pénal (partie législative) : art 226-16 à 226-24
  - Code Pénal (partie réglementaire) : art R.625-10 à R.625-13