Département de Génétique Animale

CHARTE DE BON USAGE DES RESSOURCES INFORMATIQUES DU CTIG

Version 2

Ce règlement est avant tout un code de bonne conduite. Il a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation afin d'instaurer un usage correct des ressources informatiques, avec des règles minimales de courtoisie et de respect d'autrui.

But de la Charte

La présente charte a pour but de définir les règles de bonne utilisation des ressources communes.

Ces règles relèvent avant tout du bon sens et ont pour seul but d'assurer à chacun l'utilisation optimale des ressources, compte tenu des contraintes globales imposées par leur partage.

En cas de non respect de ces règles, les responsables du CTIG se réservent le droit d'intervenir, afin que le plus grand nombre d'utilisateurs puissent bénéficier de conditions de travail les plus satisfaisantes possible.

La Charte informe également les utilisateurs sur l'état actuel de la législation française en matière de fraude informatique, ainsi que sur les sanctions pénales encourues (indépendamment des sanctions administratives qui peuvent être appliquées par les organismes de rattachement).

Définitions

Les ressources : Les ressources communes mises à disposition des utilisateurs sont les différents serveurs UNIX et le serveur Zos munis d'un large éventail de logiciels (langages, bases de données, statistiques, ...) ainsi que les serveurs de stockage et le réseau d'accès à ces équipements. La connexion au travers du réseau RENATER permet l'accès à tout ou partie des services de communication, à savoir les services Web, le transfert de fichiers et les connexions distantes sur les serveurs.

L'utilisateur : Un utilisateur est un consommateur de ressources du CTIG.

L'administrateur : Sur chaque serveur, une ou plusieurs personnes du CTIG sont administrateurs du système et disposent pour cela de droits étendus.

Le correspondant informatique : Chaque organisme ou unité de l'INRA définit un ou plusieurs correspondants informatiques chargés de dialoguer avec le CTIG, de former et informer les utilisateurs dont il a la responsabilité. En particulier, il s'assure que tout utilisateur accédant aux ressources informatiques du CTIG a pris connaissance de la présente Charte. Si la structure n'est pas en mesure de nommer un correspondant informatique, c'est son responsable qui en assume le rôle.

SNIG : Système national d'information génétique qui consolide toutes les informations collectées sur les animaux de rente par les organismes intéressés par l'amélioration génétique. Grace aux ressources mises à disposition, les utilisateurs utilisent les données qui y sont stockées dans le cadre de leurs missions et/ou autorisations explicites.

Conditions d'accès aux ressources informatiques du CTIG

L'utilisation des ressources informatiques du CTIG n'est autorisée que dans le cadre exclusif de l'activité professionnelle des utilisateurs conformément à la législation en vigueur.

Tout utilisateur rattaché à une unité du département de génétique animale de l'INRA a accès aux ressources informatiques du CTIG sur demande d'une ouverture de compte.

Pour les autres utilisateurs, une convention indiquant précisément les projets et les conditions d'utilisation doit avoir été signée entre le CTIG ou le département de génétique animale et le responsable administratif de l'utilisateur. Elle précise en particulier le nom du correspondant informatique.

Les autorisations d'utilisation des ressources informatiques du CTIG sont strictement personnelles. Elles peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée.

Droits et devoirs des utilisateurs

En cas de problème, les utilisateurs doivent demander l'aide de leur correspondant informatique.

Informations individuelles

Pour chaque nouvel utilisateur, le correspondant informatique est tenu de fournir des informations individuelles valides via le formulaire d'ouverture de compte disponible sur CTIGWiki. Il est également tenu de notifier toute modification de ces informations et en particulier toute cessation de contrat de travail.

Conditions accès

Tout utilisateur possède un compte auquel est associé un mot de passe. La remise de ces deux informations et l'acceptation de cette charte détermine un droit accès, éventuellement limité, aux ressources du CTIG pour une durée éventuellement déterminée.

Le CTIG tient à la disposition de chaque correspondant informatique la liste des utilisateurs avec les droits dont ils disposent.

Ce droit d'accès est temporaire. Il est retiré dès lors que la fonction de l'utilisateur ne le justifie plus. Il sera retiré si le comportement d'un utilisateur est en désaccord avec les règles définies dans la présente Charte.

Gestion du mot de passe

Chaque utilisateur est responsable de l'usage des ressources informatiques effectué à partir de son compte. Cela nécessite que des précautions élémentaires soient prises, en particulier :

- Adopter un mot de passe sûr gardé secret et en aucun cas ne le communiquer à des tiers même temporairement.

- Changer régulièrement son mot de passe (en particulier après chaque démonstration en public), à l'exception des comptes ftp qui sont à validité permanente.

- En fin d'utilisation d'un poste de travail, verrouiller ou fermer les sessions ouvertes, afin de ne pas laisser des ressources ou des services disponibles sans identification.

- Prévenir les administrateurs de toute tentative de violation (même non réussie) de son compte.

- Ne pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité.

Note : La tentative d'usurpation d'identité est un délit.

Respect du caractère confidentiel des informations

La possibilité de modifier un fichier n'implique pas l'autorisation de le modifier. Toute tentative de lecture ou de copie des fichiers d'un autre utilisateur sans son autorisation est donc répréhensible.

L'utilisateur doit assurer la protection de ses informations et 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 ceux mis à sa disposition. Enfin il doit signaler toute anomalie qu'il peut constater.

Utilisation des réseaux et des systèmes

L'interconnexion actuelle des systèmes permet une grande convivialité dans l'utilisation des ressources mais impose des règles strictes de bonne conduite sous peine de se voir exclure de cette communauté.

Les ressources du CTIG ne doivent pas être utilisées pour se connecter illégalement sur des systèmes distants. Par ailleurs, l'utilisateur s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès ou un mode d'emploi d'accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage.

L'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités professionnelles et dans le respect de principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur.

Les agissements suivants s'ils sont réalisés sciemment sont considérés comme des fautes graves pouvant entraîner la fermeture immédiate du compte utilisateur concerné :

- interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés,

- accéder à des informations privées d'autres utilisateurs sur le réseau,

- modifier/détruire des informations sur un des systèmes connectés,

- rendre nécessaire la mise en place de moyens humains ou techniques complémentaires pour contrôler les agissements d'un utilisateur sur le réseau,

De même, le développement, l'installation ou la simple copie sur un des serveurs du CTIG d'un programme ayant les propriétés ci-dessous est interdite :

- programmes harcelant d'autres utilisateurs

- programmes pour contourner la sécurité

- programmes saturant les ressources

- programmes virus et cheval de Troie

- programmes contournant les protections des logiciels

La copie d'un programme sous licence commercial est formellement interdite.

Utilisation des ressources communes

Le partage des ressources du CTIG par un nombre élevé d'utilisateurs ayant des besoins souvent fort différents implique le respect de quelques règles.

L'utilisation des ressources doit être rationnelle et loyale afin d'en éviter la saturation.

Un utilisateur ne doit pas avoir d'activité visant à limiter ou à interdire l'accès à des ressources communes aux autres utilisateurs.

L'utilisation de l'espace disque doit être maitrisée afin de limiter le gaspillage au minimum (nettoyage fréquent, compression, archivage, ...).

Accès aux données des SNIG et autres bases de données hébergées au CTIG

Toutes les bases de données hébergées au CTIG sont de nature privée. L'accès aux données est donc règlementé et se fait selon les préconisations de chaque SNIG (exemple : droits d'accès définis dans le cadre de FGE).

L'accès à ces données peut se faire directement à la source de stockage (base de données relationnelles) ou via des ensembles de fichiers consolidés et mis à jour régulièrement nommés BDIR (Base de Données Indexation Recherche) ou infocentre.

Dans les deux cas, l'accès est nominatif et l'utilisateur doit être dans le groupe adéquat. La demande de rattachement à un groupe peut être faite par le correspondant informatique, le responsable de la BDIR ou l'administrateur du SNIG concerné.

L'utilisateur ayant un accès s'engage à n'utiliser les données que dans le cadre de ses missions pour lesquelles il a obtenu les droits.

Toute utilisation en dehors du cadre prévu doit faire l'objet d'une demande écrite à la Direction du CTIG qui instruira la demande.

Les identifiants d'accès aux applications de consultation web sont strictement personnels et ne doivent pas être diffusés.

L'utilisateur s'engage à ne pas céder à un tiers des données dont il ne serait pas propriétaire sans l'accord du CTIG.

L'usage des données par l'utilisateur identifié n'engage pas la responsabilité du CTIG.

Droits et devoirs des administrateurs

Les administrateurs du CTIG surveillent la qualité du service. Ils font respecter les droits des utilisateurs.

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés. Le CTIG se réserve le droit de prendre toute disposition nécessaire pour assumer ces responsabilités et permettre le bon fonctionnement des ressources informatiques communes.

Disponibilité des ressources informatiques

Les administrateurs du CTIG informent les utilisateurs des interruptions volontaires de service et ils s'emploient à minimiser ces interruptions et à choisir des dates et des heures fixes.

Accès aux données privées

Les personnels du CTIG peuvent accéder à des fichiers ou courriers pour diagnostic ou correction de problème. Pour assurer la bonne marche du système ou pour vérifier l'application de la Charte, ils peuvent examiner des données appartenant à des utilisateurs. Ils doivent respecter la confidentialité des informations auxquelles ils auront accès au cours de ces démarches comme ils s'y sont engagés en signant eux-mêmes la charte des administrateurs de l'INRA.

Dans le cas où un fichier douteux ou de taille excessive est détecté, l'administrateur peut (avec ou sans préavis) l'isoler et prendra contact avec le correspondant informatique pour décider des suites à donner.

Contrôle de l'utilisation des ressources

Les personnels du CTIG peuvent surveiller en détail les sessions de travail d'un utilisateur s'il existe un soupçon de non-respect de la Charte.

Ils peuvent interrompre toute tâche utilisateur dans le cas où une utilisation excessive des ressources nuit au bon fonctionnement du système (avec ou sans préavis, selon l'urgence du problème).

Respect des restrictions légales d'utilisation

Les lois et décrets en cours de validité s'appliquent à tous.

Rappel des principales lois françaises

Il est rappelé que toute personne sur le sol français doit respecter la législation française en particulier dans le domaine de la sécurité informatique :

- la loi du 6/1/78 dite "informatique et liberté",(cf. http://www.cnil.fr/)

- la législation relative à la fraude informatique, (article 323-1 à 323-7 du Code pénal),(cf. http://www.legifrance.gouv.fr/citoyen/code.cgi)

- la législation relative à la propriété intellectuelle(cf. http://www.legifrance.gouv.fr/citoyen/code.cgi)

- la loi du 04/08/1994 relative à l'emploi de la langue française,(cf. http://www.culture.fr/culture/dglf/)

- la législation applicable en matière de cryptologie.(cf. http://www.telecom.gouv.fr/francais/activ/techno/crypto0698_1.htm) Règles d'utilisation, de sécurité et de bon usage

Protection des logiciels

Les mêmes valeurs intellectuelles s'appliquent aux logiciels et aux autres publications du monde académique (cf loi du 3/7/1985).

Dans le cas d'un logiciel protégé : toute copie est interdite même pour sauvegarde (elles sont assurées par les administrateurs).

Toute copie illicite d'un logiciel est assimilable à un vol.

Aucun code source d'un logiciel protégé ne peut être inclus dans des logiciels pouvant être utilisés à l'extérieur.

Certains logiciels ayant bénéficié d'une licence d'acquisition spéciale "éducation", des vérifications s'imposent avant leur utilisation en dehors de la communauté de la recherche.

Fraude informatique

Le texte de référence est la loi du 5/1/88 (loi Godfrain). Sont considérés comme des délits les activités suivantes :

- accès ou maintien frauduleux dans un système informatique,

- atteintes volontaires au fonctionnement d'un système informatique,

- la tentative de ces délits,

- l'association ou l'entente en vue de les commettre.

Conditions de confidentialité

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie. Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés, il devra auparavant en avoir fait la demande à la CNIL en concertation avec le Directeur du CTIG et en avoir reçu l'autorisation. Il est rappelé que cette autorisation n'est valable que pour le traitement défini dans la demande et pas pour le fichier lui-même.

Sanctions éventuelles

Le non-respect des règles de bonne conduite fixées par cette Charte, ainsi que des textes de loi en vigueur, peut conduire au déclenchement des procédures de contrôle relatives à l'utilisation des ressources informatiques de l'Inra (N/S N° 2008-53) qui peut aboutir aux sanctions précisées dans cette note de service..