|  |  |
| --- | --- |
|  | Département de Génétique Animale**US0310 CTIG** |

**CHARTE DE BON USAGE DES
RESSOURCES INFORMATIQUES DU CTIG**

**Version 3 (oct 2023)**

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 informatiques munis d'un large éventail de logiciels (langages, bases de données, statistiques, ...) ainsi que des espaces de stockage de données et le réseau d'accès à ces dispositifs. La connexion au travers du réseau Internet 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 d’INRAE identifie un ou plusieurs correspondants informatiques. Il est chargé de dialoguer avec le CTIG, de former et informer les utilisateurs dont il suit l’activité. 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.

### 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 d’INRAE a accès aux ressources informatiques du CTIG (automatiquement pour un agent du département de Génétique Animale, sur demande d’une ouverture de compte sous réserve d’un accord de son département avec le département Génétique Animale).

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 la forge DGA ou l’application dédiée. Il est également tenu de notifier toute modification de ces informations et en particulier toute cessation de contrat de travail ou modification de ses activités affectant ses droits d’accès.

#### 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 et à minima tous les ans), 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.

Il est rappelé que 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 fluidité 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 à 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, conformément à la législation en vigueur, 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.

Les actions suivantes si elles sont réalisées sciemment sont considérées 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 en contrôler les conséquences,

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 commerciale 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 bases de données hébergées au CTIG

Les bases ou dépôts de données hébergées au CTIG sont en grande majorité de nature privée. L’accès aux données est donc règlementé et se fait selon les préconisations de chaque propriétaire ou client (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, dépôt de données) ou via des ensembles de fichiers consolidés et mis à jour régulièrement nommés infocentres.

Dans les deux cas, l’accès est nominatif et l’utilisateur doit appartenir à un groupe d’accès adéquat. La demande de rattachement à un groupe peut être faite par le correspondant informatique ou le responsable de la base concernée.

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 ses responsabilités et permettre le bon fonctionnement des ressources informatiques communes.

#### Disponibilité des ressources informatiques

Les administrateurs du CTIG informent les utilisateurs des interruptions planifiées de service. Ils s'emploient à minimiser ces interruptions et à annoncer à l’avance les créneaux retenus.

#### Accès aux données privées

Les personnels du CTIG peuvent accéder à des fichiers 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 d’INRAE.

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 principaux textes réglementaires

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 janvier 1978 dite "informatique et liberté" (cf. <https://www.legifrance.gouv.fr/loda/id/LEGISCTA000006095896> )
* la législation relative à la fraude informatique, (article 323-1 à 323-7 du Code pénal),(cf. <https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719> )
* la législation relative à la propriété intellectuelle(cf. <https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006069414> )
* le règlement général sur la protection des données (RGPD) et les adaptations du droit français qui en découlent ( cf <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679> et <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952> )

#### Protection des logiciels

Les mêmes valeurs intellectuelles s'appliquent aux logiciels et aux autres publications du monde académique (cf loi du 3 juillet1985, <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000693451> ).

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

Sont considérées 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 ou du RGPD, 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 d’INRAE (N/S N° 2008-53) qui peut aboutir aux sanctions précisées dans cette note de service.