RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

INRAE

Charte d'usage des ressources informatiques

Applicable au 1er janvier 2026

Etablissement public à caractère scientifique et technologique placé sous la tutelle conjointe des ministres chargés de l'agriculture et de la recherche

Résumé

Préambule

La présente charte a pour objet de définir les droits et obligations qui président aux usages des Ressources Informatiques d'INRAE mises à la disposition des agents par INRAE.

Définitions

Est désignée « Utilisateur » la personne ayant accès ou utilisant les ressources informatiques d'INRAE, y compris quand elle n'est pas agent INRAE.

Les « Ressources Informatiques » désignent tout matériel informatique (postes de travail, terminaux mobiles, équipements réseaux, serveurs, robots, objets connectés…) et tout logiciel (système d'exploitation, application, script) qui est une composante du système d'information d'INRAE, ainsi que tout contenu ou donnée stockés même temporairement dans ce système d'information mis à disposition de l'Utilisateur par INRAE dans le cadre de ses activités professionnelles.

Périmètre d'application

La charte s'applique à tout Utilisateur des Systèmes d'Information et de communication d'INRAE et des Ressources Informatiques mises à sa disposition par INRAE.

Usage professionnel des Ressources Informatiques INRAE

L'Utilisateur est responsable du bon usage des Ressources Informatiques mises à sa disposition, des moyens d'authentification qui lui sont fournis et de la protection des informations qu'il manipule.

À son poste de travail sur site, en télétravail, comme lors de tous ses déplacements, trajets quotidiens comme missions, en France comme à l'étranger, l'Utilisateur veille à la mise en œuvre des recommandations fournies par INRAE en matière de cybersécurité quant à l'utilisation :

- de son poste de travail informatique ;
- de sa messagerie professionnelle ;
- des outils de visioconférence et de messagerie instantanée ;
- des réseaux et des services numériques sur Internet, incluant l'usage des intelligences artificielles génératives (IAG).

Il adapte le niveau de protection des informations qu'il manipule selon les prescriptions fournies par les instructions ministérielles. Il accepte par ailleurs les moyens de protection face aux menaces déployés par INRAE.

L'Utilisateur signale immédiatement au support informatique tout dysfonctionnement constaté, toute perte, vol ou détérioration de matériel.

En cas de départ d'INRAE, l'Utilisateur restitue tous les matériels professionnels mis à sa disposition et s'assure de la transmission de ses données professionnelles afin d'en assurer la préservation et de garantir la continuité de service.

Protection des données à caractère personnel et de propriété intellectuelle

L'Utilisateur s'engage au respect de la réglementation applicable en matière de propriété intellectuelle et de traitement de données à caractère personnel.

INRAE s'engage au respect de la confidentialité et de la sécurité des données des utilisateurs bénéficiaires de ressources et outils numériques INRAE et veille à permettre l'exercice de leurs droits.

Usage de Ressources Informatiques personnelles ou à titre privé

Un usage à titre privé des Ressources Informatiques fournies par INRAE est toléré sous conditions. En l'absence de mesure spécifique prise par l'Utilisateur, toute information stockée en utilisant ces Ressources Informatiques est réputée à usage professionnel.

Les matériels personnels n'ont pas vocation à être raccordés aux réseaux INRAE ni à être utilisés dans un cadre professionnel. Des aménagements existent, notamment concernant la messagerie professionnelle, mais sous réserve du respect de certaines consignes.

L'utilisation de services numériques personnels à des fins professionnelles est quant à elle interdite, sauf exceptions décrites dans la présente charte.

Empreinte environnementale du numérique

En cohérence avec sa stratégie de responsabilité sociétale et environnementale (RSE), INRAE est attentif aux impacts de ses activités notamment en matière numérique.

L'Utilisateur s'engage à ce titre à adopter des pratiques visant à réduire son empreinte environnementale. Elles concernent notamment l'achat de matériel, l'utilisation des ressources et la gestion des déchets électroniques.

L'Utilisateur veille par ailleurs au respect des bonnes pratiques relatives à son équilibre entre vie personnelle et vie professionnelle et à un usage responsable des outils numériques.

Sensibilisation des utilisateurs aux usages et à la sécurité numériques

L'Utilisateur est sensibilisé aux enjeux de la sécurité numérique. Il s'engage à en observer les règles et recommandations. Il associe également les bonnes pratiques édictées par INRAE en matière d'expression publique des agents INRAE. L'Utilisateur signale à son support informatique tout comportement anormal de son matériel et tout risque de vol ou perte de données.

Dispositions spécifiques aux personnels à privilèges élevés

L'Utilisateur qui, compte tenu de son affectation ou de sa mission, dispose d'un large accès aux systèmes d'information, aux ressources et aux données, ou de privilèges élevés nécessaires à leur gestion, bénéficie de droits d'intervention plus étendus en échange de quoi il s'engage à observer des obligations particulières en termes de sécurité, de discrétion professionnelle et de confidentialité.

Table des matières

I. Préambule

La présente charte a pour objet de définir les droits et obligations des Utilisateurs de Ressources Informatiques.

Ces règles ont pour finalité de contribuer à la protection de l'Utilisateur, à la préservation de la sécu-rité des systèmes d'information d'INRAE, de garantir la disponibilité, l'intégrité et la confidentialité des données qui y sont hébergées et préserver la responsabilité de l'Institut vis-à-vis des tiers. Tout manquement aux règles qui régissent la sécurité des systèmes d'information est en effet susceptible d'avoir des impacts importants (humains, financiers, juridiques, environnementaux, atteinte au fonctionnement de l'organisme ou au potentiel scientifique et technique).

Les obligations des Utilisateurs prévues par la présente charte ont un caractère opposable. Tout man-quement, selon sa gravité, est susceptible d'entraîner pour l'Utilisateur des sanctions disciplinaires, et ce sans préjudice d'éventuelles actions pénales ou civiles à son encontre.

Ce document a pour ambition de conduire à l'adoption des bonnes pratiques d'utilisation des Ressources Informatiques et d'accompagner l'évolution des usages numériques et de la réglementation.

Enfin, l'usage raisonné des Ressources Informatiques concourt par ailleurs à une conciliation saine et équilibrée des temps de vie professionnel et personnel.

Pour faciliter sa lecture, les noms employés dans cette charte pour désigner des fonctions, des métiers ou des responsabilités (porteur de projet, chercheur, directeur d'unité…) sont employés au sens générique et ont une valeur neutre.

II. Définitions

« **Utilisateur** » : désigne la personne ayant accès ou utilisant les Ressources Informatiques qu'il s'agisse ou non d'un « Utilisateur Externe ».

« **Utilisateur Externe** » : désigne toute Utilisateur qui n'est pas un personnel INRAE (personnels de partenaires, prestataires…).

« **Administrateur** » : désigne tout Utilisateur qui dispose, par sa fiche de poste ou au titre d'une mission spécifique, d'accès particuliers au Système d'Information d'INRAE, lui conférant des privilèges élevés, des accès larges aux systèmes et/ou aux données. Ce personnel peut être technique (Informaticien de Proximité, ingénieur informatique…) ou fonctionnel (responsable d'une application).

Les Administrateurs sont des Utilisateurs et se voient appliquer les règles applicables à ceux-ci sous réserve des modalités spécifiques relative à leur fonction d'Administrateur décrites dans la présente Charte.

« **Ressource Informatique** » : désigne tout matériel informatique (postes de travail, terminaux mobiles, équipements réseaux, serveurs, robots, objets connectés …) et tout logiciel (système d'exploitation, programme, application…) qui est une composante d'un Système d'Information d'INRAE ainsi que tout contenu ou donnée stockés même temporairement dans ce système d'information dès lors qu'ils sont mis à disposition de l'Utilisateur par INRAE dans le cadre de ses activités professionnelles.

Ces Ressources Informatiques sont protégées par la politique de sécurité des systèmes d'information (PSSI) d'INRAE qui s'étend sur tous les Systèmes d'Information (SI) tels que définis ci-dessous.

Le « **Système d'Information** » recouvre l'ensemble des infrastructures et services logiciels informatiques permettant de collecter, traiter, transmettre et stocker les données sous forme numérique sous la responsabilité et/ou le contrôle d'INRAE. Ils

comprennent les données d'INRAE et des partenaires hébergées dans des infrastructures tierces telles que des services de stockage en ligne. L'informatique nomade, telle que les ordinateurs portables, les terminaux mobiles, les ordiphones…, est également un des éléments constitutifs du Système d'Information d'INRAE.

Un « **Matériel Personnel »** est un équipement détenu par l'Utilisateur qui n'est pas mis à disposition par l'employeur et capable d'interagir avec les Systèmes d'Information ou de se connecter aux Ressources Informatiques. Le Matériel inclut ordinateur, ordiphone, tablette, stockage amovible, objets connectés personnels (montres, lunettes…), etc.

La « **Politique de Sécurité des Systèmes d'Information** » (PSSI) définit les objectifs et les principes en matière de sécurité du numérique sur les périmètres institutionnel et d'unité, elle explicite la gouvernance de la sécurité numérique et sa mise en œuvre dans les unités.

On entend par « **protection** » d'une Ressource Informatique tout comportement ou toute mesure attendue de l'Utilisateur pour prévenir, limiter ou remédier à l'atteinte à la confidentialité, l'intégrité ou la disponibilité d'une Ressource Informatique sur la base des recommandations formulées par la PSSI et de la présente charte, ou sur la base du comportement raisonnable que l'on peut attendre de toute personne dans une situation donnée. Le terme « protection » s'étend aussi aux mesures mises en œuvre par l'établissement pour les mêmes finalités.

« **Privilège** » : délégation d'autorité sur un système informatique accordé à un Utilisateur lui permettant d'effectuer une action donnée.

III. Modalités d'application

La présente charte s'applique à tout Utilisateur des Systèmes d'Information d'INRAE. S'agissant des Utilisateurs Externes, la charte leur est applicable sous réserve des devoirs spécifiques aux personnels INRAE (droit à la déconnexion, achat de matériel informatique, communication…).

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

Elle est systématiquement présentée à chaque nouvel agent recruté ou accueilli. Lors de sa première connexion au Système d'Information, celui-ci atteste en avoir pris connaissance.

Tout contrat prévoyant l'accès aux Ressources Informatiques par des tiers (exemple : contrat de prestation, convention de partenariat ou de recherche…) doit inclure l'engagement par les représentants légaux de ces tiers de respecter et de faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes sous leur responsabilité qui seraient Utilisateurs.

Cette charte s'inscrit dans le cadre de la mise en œuvre la politique générale de sécurité des systèmes d'information (PGSSI) et la politique opérationnelle du système d'information (POSSI) d'INRAE qui prévalent en cas de contradiction.

Si des dispositions légales ou réglementaires postérieurement adoptées entrent en contradiction avec cette charte, l'application de ces dispositions prévaudront sur elle.

Cette charte constitue un complément à d'autres chartes, notes de service et documents qui peuvent aborder l'utilisation des moyens numériques, qu'ils soient mentionnés ou non dans la charte.

IV. Principes de sécurité

Les recommandations générales de sécurité numérique sont disponibles sur le site intranet INRAE dédié à la cybersécurité.

IV.1. Sensibilisation de l'Utilisateur

L'Utilisateur est informé de la nécessité d'acquérir les bases essentielles de la sécurité numérique ou de ce que tout un chacun devrait connaître pour faire face à une menace grandissante. Il lui est donc demandé de suivre le parcours de sensibilisation à la sécurité numérique proposé sur la plateforme de e-formation d'INRAE.

IV.2. Protection des informations et des documents électroniques

Dans le cadre de ses fonctions, l'Utilisateur doit connaître le niveau de sensibilité des informations qu'il manipule. Il se réfère pour cela à l'échelle de sensibilité de l'information disponible sur le site intranet dédié à la cybersécurité. L'Utilisateur est responsable de la protection des informations qu'il adapte en fonction de leur degré de sensibilité. Conformément à la PSSI, il indique le niveau de confidentialité des documents qu'il crée en respectant l'échelle de sensibilité définie et respecte le marquage des documents qui lui sont transmis.

Ainsi, l'Utilisateur s'interdit de transmettre des données sensibles (exemples : données du secret de la défense nationale, données sensibles non classifiées de défense) aux personnes non autorisées. Toute transmission autorisée de données sensibles en application d'une disposition légale ou réglementaire spécifique doit être réalisée suivant les règles de protection en vigueur prescrites dans la réglementation et les consignes applicables.

IV.3. Messagerie

Tout Utilisateur doit utiliser l'adresse électronique professionnelle qui lui a été attribuée à sa prise de fonction. La messagerie mise à disposition de l'Utilisateur est destinée à un usage professionnel. L'utilisation de la messagerie électronique au sein d'INRAE doit respecter les règles établies pour garantir la sécurité et la conformité des communications mentionnées notamment dans le présent document et sur le site intranet dédié à la cybersécurité.

Il est également crucial de faire preuve de vigilance face aux hameçonnages. L'Utilisateur doit être attentif aux courriels suspects, vérifier l'identité de l'expéditeur, et ne pas cliquer sur des liens ou télécharger des pièces jointes provenant de sources inconnues ou non vérifiées.

La redirection de la messagerie est autorisée uniquement vers les messageries professionnelles des partenaires académiques français d'INRAE.

Sur les téléphones et postes de travail professionnels, seules les applications de messagerie recommandées par INRAE sont autorisées. L'utilisation d'agrégateurs de messagerie en ligne qui permettent d'ajouter l'adresse professionnelle de l'Utilisateur est interdite.

L'Utilisateur est informé que le courriel est reconnu comme un document pouvant servir de preuve en cas de contentieux. Par conséquent, il est essentiel que l'Utilisateur soit prudent quant à la nature des informations échangées par voie électronique, de la même manière que pour les courriers traditionnels.

IV.4. Protection des accès aux informations

Les moyens d'authentification constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Ainsi l'Utilisateur assure la protection des moyens d'authentification qui sont strictement personnels et qui lui ont été affectés ou qu'il a générés (badges, mots de passe, clés de sécurité, certificats, etc.). Il ne les confie jamais à un tiers et s'engage à

restituer les moyens physiques d'authentification à la fin de ses fonctions. Les équipes INRAE dédiées ne demanderont jamais la communication des mots de passe.

L'Utilisateur informe les Administrateurs du système d'information de toute évolution de ses fonctions nécessitant une modification de ses droits d'accès qui n'aurait pas été prise en compte. L'Utilisateur signale les accès qu'il aurait obtenus par erreur.

L'Utilisateur n'accède pas, ne tente pas d'accéder, ne supprime ou ne modifie pas des informations qui ne relèvent pas de ses missions.

L'Utilisateur signale à la chaîne fonctionnelle SSI toute violation ou tentative de violation suspectée de son compte. Il signale tout cas de perte, de vol ou de détérioration du matériel. De manière générale, il signale tout dysfonctionnement à son support informatique de proximité.

IV.5. Protection des Ressources Informatiques

L'Utilisateur doit activer les moyens de protection mis à sa disposition, tels que la sauvegarde, la mise sous clé, le verrouillage du poste de travail, etc. Il est plus généralement tenu de mettre en œuvre les recommandations en matière de cybersécurité.

La présence d'une solution de protection contre les codes malveillants, fournie par INRAE, est obligatoire sur tous les équipements et ne peut en aucun cas être désactivée.

Si le chiffrement est mis en œuvre sur des contenus possédés ou manipulés par l'Utilisateur, celui-ci doit fournir à INRAE les moyens de les déchiffrer en cas de besoin.

L'Utilisateur est informé qu'afin de satisfaire à ses obligations réglementaires, INRAE doit mettre en œuvre des conditions d'administration pour lui permettre d'assurer la protection du SI et la détection de tentatives de compromission et d'activités illicites. Ces conditions d'administration peuvent prendre des formes diverses qui restent toutes dans les limites définies par le droit du travail, le règlement général sur la protection des données (RGPD) et la loi Informatique et Libertés modifiée.

Parmi elles, sont déployés :

- Des systèmes automatiques de filtrage : du filtrage d'URL est opéré sur les équipements réseaux des sites et au niveau des postes de travail. Ce filtrage se fait sur la base de la réputation web. Ces mécanismes n'assurent pas une protection absolue et ne dédouanent pas l'Utilisateur d'être vigilant dans son utilisation d'Internet ;
- Des systèmes automatiques dédiés à la traçabilité des actions : toutes les connexions sur les SI INRAE ou hors INRAE (et notamment logiciels, serveurs, équipements réseaux, matériels de travail professionnels) sont conservées à des fins d'analyse en cas d'anomalie sur une durée de 12 mois. Ce délai passe à 5 ans dans le cas de suivi de vulnérabilités et incidents de sécurité identifiés, sauf procédure judiciaire (conservation le temps de la procédure). Des outils de détection d'intrusion et de compromission qui peuvent identifier des usages anormaux sont également déployés ;
- Des systèmes de gestion du poste de travail : tous les postes de travail sont inventoriés (matériel, logiciels et Utilisateurs associés) et les informations partagées auprès des personnes en charge du suivi de ces postes. Les matériels de travail professionnels peuvent être réquisitionnés pour analyse par les personnes habilitées dans les cas suivants :
  - en cas d'incidents de sécurité, de constat ou de suspicion d'actes non conformes à cette charte dans les conditions prévues par la note de service relative aux contrôles des usages non conformes des Ressources Informatiques (cf. annexe) ;

- en cas d'indices graves et concordants rendant vraisemblable la commission d'une infraction, ou afin d'assurer une continuité dans l'activité professionnelle en cas d'absence de l'agent dans les conditions prévues par la loi.

IV.6. Protection vis-à-vis des échanges sur les réseaux

L'Utilisateur fait preuve de vigilance vis-à-vis de la provenance et du contenu des informations qu'il reçoit (désinformation, virus informatique, tentative d'escroquerie, chaînes, hameçonnage…) que ce soit par courriel, par messagerie instantanée, par téléphone, par SMS ou tout autre moyen de communication. Il en est de même pour les informations reçues sous forme de fichiers audio ou vidéo qui peuvent avoir été générées par des intelligences artificielles.

Si une utilisation résiduelle privée est tolérée, il est rappelé que les connexions établies grâce aux Ressources Informatiques mises à disposition par INRAE sont présumées avoir un caractère professionnel.

IV.7. Protection vis-à-vis des services numériques sur Internet

L'Utilisateur s'interdit d'utiliser ses coordonnées professionnelles, en particulier son adresse électronique ou autre identifiant, sur des services sans rapport avec son activité professionnelle. En contrevenant à cette consigne, il facilite les atteintes à sa réputation, à la réputation de l'unité ou à celle d'INRAE.

L'usage de services numériques sur Internet (Cloud, Intelligence Artificielle Générative (IAG)…) à des fins professionnelles se fait avec ses coordonnées professionnelles et respecte les consignes d'usage données par l'établissement.

L'Utilisateur doit s'informer des Conditions Générales d'Utilisation et prendre en considération la sensibilité des données manipulées avant tout usage éventuel d'un service numérique en ligne.

Certains sites malveillants profitent de failles logicielles pour récupérer les données présentes sur le poste de travail. D'autres sites mettent à disposition des logiciels qui, sous une apparence anodine ou dissimulés dans d'autres, peuvent prendre le contrôle de l'ordinateur et transmettre son contenu au pirate à l'insu de l'Utilisateur.

Par conséquent, l'Utilisateur :

- Évite de se connecter à des sites suspects et ne télécharge des contenus numériques que sur des sites de confiance ;
- S'interdit de télécharger des logiciels qui n'ont pas été validés par l'unité ;
- N'opère les sauvegardes de données, les partages d'informations, les échanges collaboratifs, que sur des sites de confiance, mis à disposition par l'établissement ou une des tutelles de l'unité et dont la sécurité a été vérifiée par l'établissement ;
- Ne diffuse aucune information interne à INRAE sur un service numérique sur Internet (blog, forum, réseaux sociaux…).

IV.8. Visioconférence et messagerie instantanée

L'usage des services de visioconférence et de messagerie instantanée nécessite une attention particulière. En particulier, certains outils sont adaptés pour des échanges sensibles, au contraire d'autres services. L'Utilisateur doit donc sélectionner la solution adaptée en fonction de la sensibilité de ses échanges. De même, il doit veiller à sécuriser convenablement ses visioconférences ou ses salons de discussions (invitation, salle d'attente, mot de passe d'accès…) en fonction des besoins de sécurité.

IV.9. Missions et nomadisme

La vigilance est de mise lors des déplacements et trajets quotidiens : il est important de rester attentif à ses matériels. L'Utilisateur doit s'abstenir de travailler sur des documents ou contenus sensibles dans les lieux publics ou lors des déplacements s'il n'utilise pas un filtre de confidentialité pour éviter les regards indiscrets. Un câble antivol peut être aussi utilisé pour sécuriser physiquement les équipements.

Les départs en mission, qu'ils soient en France, en Europe ou au-delà, nécessitent une vigilance accrue en matière de sécurité numérique. L'Utilisateur doit impérativement respecter les règles relatives aux missions, notamment à l'étranger, telles que détaillées dans les recommandations disponibles sur la page dédiée du site intranet relatif à la cybersécurité.

Pour les voyages en dehors de l'espace Schengen, le transfert préalable des données sur un espace collaboratif d'INRAE puis leur téléchargement une fois arrivé à destination est fortement recommandé. Cela peut impliquer de voyager avec du matériel dédié à la mission notamment vers les pays susceptibles de saisir le matériel lors de contrôles. Ces mesures visent à garantir la confidentialité et l'intégrité des informations, tout en permettant une continuité de travail sécurisée en situation de nomadisme.

L'usage des réseaux Wifi publics (hôtel, gare…) nécessite impérativement l'usage du VPN.

Le télétravail, lorsqu'il est autorisé, doit être exercé selon des mêmes règles de sécurité que celles appliquées sur site. Une vigilance accrue est de mise pour protéger les données sensibles, en minimisant les informations transportées et en chiffrant les disques, conformément aux directives de la PSSI.

IV.10. Utilisateurs disposant des privilèges d'administration de leur poste de travail

L'Utilisateur disposant d'une capacité d'administration de son poste s'engage à respecter le guide des bonnes pratiques essentielles des Administrateurs de poste de travail disponible sur le site Intranet de la cybersécurité.

V. Protection des données à caractère personnel

V.1. Protection des données à caractère personnel par l'Utilisateur

L'Utilisateur est informé de la nécessité de respecter la réglementation en matière de traitements (automatisés ou non) de données à caractère personnel, conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée. Il lui est donc recommandé de suivre le parcours de sensibilisation au RGPD proposé sur la plateforme de e-formation d'INRAE.

Une donnée à caractère personnel est une information relative à une personne physique susceptible d'être identifiée directement ou indirectement.

Tout traitement impliquant des données à caractère personnel créé par un Utilisateur doit être conforme aux dispositions du RGPD et de la loi n°78-17 précitée et doit suivre la politique de protection des données de l'établissement. Sont notamment considérées comme des traitements les opérations suivantes : l'enregistrement, la conservation, la diffusion de données à caractère personnel sur support numérique ou papier.

En conséquence, tout Utilisateur souhaitant procéder à un traitement (par exemple projet scientifique, système de vidéosurveillance, nouveau traitement lié à la gestion des RH, etc.) devra en informer préalablement le responsable de traitement ainsi que le délégué Informatique et Libertés (DIL) et suivre les mesures nécessaires au respect des dispositions légales (notamment établissement d'une fiche de registre, mesures d'information des personnes concernées, mesures de

sécurité) indiquées dans la note de service relative aux modalités d'application de la réglementation relative à la protection des données à caractère personnel au sein de l'Institut et sur le site intranet Informatique et libertés - Données personnelles.

Tout Utilisateur s'engage à signaler, dès qu'il en a connaissance, toute violation de données à caractère personnel que son traitement viendrait à subir en informant l'équipe protection des données (cil-dpo@inrae.fr) et la mission cybersécurité (rssi@inrae.fr).

V.2. Protection des données à caractère personnel des Utilisateurs

Dans le cadre de l'accès et de l'utilisation des moyens informatiques et outils numériques, des données à caractère personnel de l'Utilisateur sont manipulées par INRAE. Ce dernier s'engage à respecter la confidentialité et la sécurité de ces données, conformément au RGPD et à la loi n°78-17 précitée.

Chaque Utilisateur bénéficiaire de Ressources Informatiques d'INRAE peut consulter l'information dédiée au traitement de ses données et exercer ses droits comme indiqué sur le site intranet Informatique et libertés - Données personnelles.

VI. Vie privée et Ressources Informatiques personnelles

VI.1. Usage personnel

Un usage personnel des Ressources Informatiques est toléré à condition qu'il reste de courte durée, qu'il n'affecte pas l'usage professionnel pour lequel elles ont été confiées à l'Utilisateur, le fonctionnement normal des services, et qu'il ne poursuive pas un but lucratif. Par ailleurs, comme tout usage de Ressources Informatiques à des fins professionnelles, l'usage personnel ne doit pas mettre en danger le bon fonctionnement et la sécurité du système d'information, ni enfreindre la loi, les règlements et les dispositions internes d'INRAE.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'Utilisateur comme relevant de sa vie privée. Il appartient à l'Utilisateur de procéder au stockage de ses données à caractère privé dans un espace prévu à cet effet et identifié sans ambiguïté comme tel.

Ainsi, tout Utilisateur manifestera le caractère extra-professionnel d'une partie de ses données en adoptant, exclusivement, les termes « privé » ou « personnel » pour nommer le dossier de fichiers ou l'objet du message contenant ces informations.

De même, il utilisera le terme « syndicat » pour désigner les contenus relatifs à une activité syndicale.

VI.2. Usage par les organisations syndicales

Les conditions et modalités d'utilisation des Ressources Informatiques par les organisations syndicales sont fixées par une note de service dédiée (cf. annexe).

VI.3. Usage du Matériel Personnel

L'Utilisateur s'interdit d'utiliser dans un cadre professionnel un Matériel Personnel ou de le raccorder aux réseaux INRAE (filaire ou Wifi).

Une tolérance est donnée pour accéder à la messagerie (vers l'application Web, via un navigateur en mode « navigation privée », sans enregistrer le mot de passe) et à l'Intranet institutionnel depuis un Matériel Personnel. Cet usage doit rester exceptionnel et uniquement lors d'une situation particulière justifiant l'utilisation du Matériel Personnel. Une tolérance est

aussi donnée dans le cadre de dispositifs nationaux particuliers : par exemple, diffusion d'alerte ou situation de crise. Il n'est aucunement permis d'exporter des données ou des documents internes sur le Matériel Personnel.

Dans le cadre de cette tolérance, l'Utilisateur est autorisé à connecter un équipement personnel uniquement sur les réseaux autorisés mentionnés sur le site intranet cybersécurité avec un compte invité et non le compte d'agent INRAE.

VI.4. Usage de services numériques personnels

L'utilisation de services numériques personnels à des fins professionnelles est interdite. Il n'est pas permis d'utiliser un espace de stockage en ligne (« Drive »), un service d'infrastructure (type hébergement Web, stockage, calcul…), un gestionnaire de secrets (gestionnaire de mots de passe en ligne) ou tout autre service acquis à titre personnel.

VI.5. Gestion des départs

Les Ressources Informatiques mises à disposition par INRAE sont et demeurent la propriété d'INRAE. À ce titre, l'Utilisateur est tenu de les restituer à la personne en charge de la gestion du parc informatique et/ou de la téléphonie de son unité à la date de fin de ses fonctions.

Il appartient à l'Utilisateur de détruire, selon les bonnes pratiques en vigueur, les données personnelles le concernant sur les Ressources Informatiques, préalablement à son départ.

Les personnels non-INRAE (partenaires, prestataires...) doivent également réaliser la suppression des données INRAE sur leurs matériels dès la fin de leur mission.

En cas de circonstances exceptionnelles (départ impromptu ou décès) ou si l'Utilisateur n'a pas procédé à la destruction des données personnelles le concernant, INRAE ne conserve les espaces de données à caractère privé présents sur les Ressources Informatiques que pour une période de 6 mois maximum.

L'Utilisateur doit veiller, avec son responsable, à garder accessibles à INRAE ou le cas échéant à transmettre ses données professionnelles afin notamment de garantir la continuité de service.

Les données professionnelles restent à la disposition de l'employeur. Les mesures de conservation des données professionnelles sont définies par les unités et nationalement par INRAE.

VII. Droit à la déconnexion

Les consignes INRAE sont décrites dans la charte du droit à la déconnexion d'INRAE applicable aux Utilisateurs qui ne sont pas des Utilisateurs Externes.

VIII. Empreinte environnementale du numérique

L'empreinte environnementale du numérique est principalement due à la fabrication des équipements informatiques et dans une moindre mesure à leur consommation d'énergie. Au travers de la démarche « INRAE Bas Carbone », entre autres, INRAE est engagé dans la réduction de cette empreinte environnementale. Par cette charte, l'Utilisateur s'engage à y contribuer activement.

VIII.1. Achat de matériels numériques

L'Utilisateur s'engage à adopter des pratiques visant à réduire l'achat de matériel neuf en cohérence avec les dispositions applicables en matière d'anti-gaspillage et d'économie circulaire :

- Réduire le nombre d'équipements individuels (écrans, ordinateurs, etc.) au plus juste de ses besoins ;
- Garder ses équipements individuels le plus longtemps possible (entretien, garanties) pour réduire l'achat de matériel neuf ; en cas de renouvellement anticipé, par exemple pour des enjeux de cybersécurité, favoriser le réemploi du matériel plutôt que le recyclage ;
- Réparer en première intention plutôt que de renouveler systématiquement par du matériel neuf, voire acquérir du matériel reconditionné lorsque les marchés le permettent ;
- Dimensionner son matériel au plus juste de ses besoins ;
- Privilégier les équipements mutualisés s'ils existent ;
- Favoriser la seconde vie des équipements en interne lorsque l'on n'en a plus l'utilité.

VIII.2. Utilisation des matériels et services numériques

L'Utilisateur s'engage à utiliser efficacement les Ressources Informatiques pour éviter le gaspillage de ressources, entre autres, énergétiques :

- Réduire le volume de ses données en supprimant régulièrement celles qui sont inutiles ou sauvegardées ailleurs ;
- Remobiliser des données existantes lorsqu'elles existent plutôt que d'en générer de nouvelles ;
- Privilégier les outils de partage de données (outils collaboratifs institutionnels ou d'unité) plutôt que des sauvegardes en multiples copies ;
- Limiter l'usage des assistants IA au strict nécessaire ;
- Limiter la quantité de calcul sur les infrastructures numériques au strict nécessaire ;
- Utiliser des outils et moteurs de recherche responsables lorsqu'ils existent ;
- Adopter les bonnes pratiques en matière d'envoi et de gestion des mails

VIII.3. Gestion des déchets électroniques

L'Utilisateur doit respecter la politique de recyclage et de gestion des déchets électroniques (DEEE) d'INRAE en s'appuyant sur les services organisés par son unité ou son centre. Les règles de mises au rebus, y compris pour le recyclage ou la revalorisation, imposent par exemple l'effacement sécurisé des données au préalable.

IX. Communication

La communication numérique, en tant qu'activité professionnelle, doit être conforme aux valeurs, aux exigences de qualité scientifique et aux attentes de la société, dans le respect des règles internes de l'établissement.

À ce titre, l'Utilisateur est invité à :

- Consulter et appliquer les recommandations en matière de communication responsable, visant à limiter l'impact environnemental des actions de communication (réduction des envois inutiles, choix de supports adaptés, etc.) ;

- Prendre connaissance de la Charte d'expression publique, qui définit les principes à respecter lors de toute prise de parole ou publication à titre professionnel, afin de garantir la cohérence et la qualité des communications d'INRAE.

En communiquant au nom d'INRAE, vous vous engagez également à produire des contenus en accord avec la charte graphique INRAE et en appliquant les règles typographiques en vigueur. Il est important que l'ensemble des communications, peu importe le support, soit harmonieux et respectueux de ces guides, codes et normes.

X. Propriété intellectuelle

L'utilisation des moyens informatiques et outils numériques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et, plus généralement, de tous tiers titulaires de tels droits. L'usage ou même le téléchargement de contenus numériques sans licence (logiciels, images, vidéos, textes, données…) fait courir des risques juridiques, financiers et de sécurité à INRAE.

En conséquence, chaque Utilisateur doit :

- Utiliser les logiciels, bases de données, pages web, textes, images, vidéos, photographies ou autres créations protégées par le droit de la propriété intellectuelle dans le strict respect des licences qui leur sont attachées ;
- S'abstenir d'utiliser, reproduire, copier, diffuser, modifier, sans avoir obtenu préalablement, si requis, l'autorisation du ou des titulaires des droits de propriété intellectuelle.

XI. Dispositions spécifiques aux Administrateurs

XI.1. Attributions d'un Administrateur

En application des consignes qui lui ont été transmises, l'Administrateur peut prendre toute disposition nécessaire afin d'assurer le bon fonctionnement et la sécurité des composants des Systèmes d'Information dans son périmètre de responsabilité tels que désignés dans sa fiche de poste.

En particulier, il peut :

- Isoler, suspendre ou reconfigurer des comptes utilisateurs, équipements ou applications informatiques pouvant compromettre la sécurité du système d'information ; lorsque la situation l'exige il demande l'autorisation de son supérieur hiérarchique ou du Responsable de la sécurité des systèmes d'information (RSSI) ;
- Procéder à des vérifications techniques, manuelles ou outillées, sur les fichiers et bases de données, la messagerie, les connexions à Internet, les fichiers de journalisation, etc., afin de déceler et traiter toute anomalie ou incident de sécurité qui pourrait porter atteinte au bon fonctionnement et à la sécurité des systèmes d'information dans les activités d'administration et d'assistance ;
- Traiter (détection, analyse, éradication, filtrage, etc.) ou s'assurer du traitement de tout évènement informatique présentant des risques de sécurité (par exemple : virus, intrusion, utilisation d'un logiciel interdit ou potentiellement dangereux, etc.). L'Administrateur peut alerter le RSSI de toute utilisation de Ressources Informatiques qui apparaîtrait comme non conforme à la présente charte ou à la PSSI.

Il ne peut être contraint par son responsable hiérarchique, par tout agent INRAE ou par tout tiers à enfreindre la loi : ainsi, il doit refuser de faire un contrôle ou une action qui ne respecte pas les obligations légales ou les droits élémentaires des Utilisateurs.

XI.2. Obligations d'un Administrateur

Tout Administrateur est soumis à une obligation de confidentialité et de non divulgation liée à ses activités. C'est pourquoi :

- Les permissions d'administration attribuées à un Administrateur ne sont utilisées que pour mener à bien les tâches qui lui sont confiées ;
- L'Administrateur prend connaissance des informations contenues dans les systèmes d'information ou donne accès à celles-ci seulement dans le cadre de ses fonctions et/ou sur demande explicite de son responsable ou en son absence du RSSI ;
- Le devoir de discrétion professionnelle lui impose l'interdiction absolue de faire état publiquement du détail de ses missions ou de ses fonctions ;
- Les outils mis à sa disposition ne sont utilisés que dans un but professionnel d'administration, supervision, exploitation, maintenance ou assistance ;
- Il ne peut prendre connaissance ou tenter de prendre connaissance du contenu des répertoires, fichiers ou message manifestement et explicitement désignés comme personnels qu'en présence de l'agent et avec son autorisation expresse, sauf en cas d'urgence justifiée nécessaire vis-à-vis de la législation ou de la sécurité ;
- Il s'engage à ne pas faire état ni utiliser les informations qu'il peut être amené à connaître dans le cadre de ses fonctions à des fins autres que la réalisation de ses missions ;
- En cas d'assistance, il ne prend en main, à distance, le poste de travail d'un Utilisateur qu'avec l'autorisation explicite de ce dernier et ne se connecte qu'aux seules ressources nécessaires à l'accomplissement de sa mission d'assistance ;
- Il a le devoir de ne pas abuser de ses prérogatives ; les contrôles réalisés doivent être faits non seulement en toute transparence mais aussi de manière proportionnée et adaptée à la finalité présentée à l'Utilisateur lors de l'information préalable à ces contrôles ;
- Il évite tout conflit pouvant exister entre ses intérêts personnels et ceux du service, il informe sa hiérarchie de tout conflit d'intérêt dans lequel il pourrait être impliqué pouvant altérer l'efficacité de sa mission ;
- Il documente ses actions et interventions de telle sorte que ses collaborateurs ne soient pas dans un état de dépendance en cas d'absence ou lorsqu'il quitte sa fonction.

De plus, l'Administrateur observe strictement les règles de sécurité et les limites fixées à ses interventions :

- Il respecte et fait respecter strictement la PSSI et les dispositions légales et réglementaires concernant le Système d'Information ;
- Il limite ses actions aux Ressources Informatiques dont il a la charge et dans le respect de la finalité de sa mission ; par ailleurs, il ne modifie les configurations et les droits d'accès que dans les cas préalablement définis ;
- Il ne prend pas ses consignes d'une personne non habilitée et fait remonter auprès de son supérieur direct tel que mentionné dans sa fiche de poste et au RSSI toute requête lui paraissant inappropriée ou contraire à la réglementation ; en cas de requête qui lui semblerait non appropriée présentée par sa hiérarchie, il est tenu d'expliquer à celle-ci les raisons de son opposition ; si cette requête était maintenue, il prévient le RSSI ;
- Il traite en première priorité toute violation des règles SSI et tout incident de sécurité qu'il est amené à constater, puis il informe sans délai le RSSI selon la procédure prévue par la chaîne fonctionnelle de sécurité. L'Administrateur peut ainsi être conduit à communiquer des informations confidentielles ou soumises au secret des correspondances dont il aurait eu connaissance, si elles mettent en cause le bon fonctionnement des systèmes d'information ou leur sécurité, ou si elles tombent dans le champ de l'article 40 alinéa 2 du code de procédure pénale ;

- Il observe les règles de sécurité en vigueur visant à protéger l'utilisation des comptes et des droits d'administration privilégiés qui lui ont été attribués ; il veille notamment à la protection des postes de travail à partir desquels il exerce ses fonctions et à la gestion des identifiants et secrets d'authentification des comptes privilégiés. Il est rappelé que les accès confiés à un Administrateur sont confidentiels et incessibles ;
- Il n'utilise ses comptes privilégiés que pour les activités et besoins directement liés aux tâches d'administration, d'exploitation ou d'assistance dont il a la charge, sachant que toute action sur les Systèmes d'Information est traçable et imputable grâce à la journalisation dont ces derniers font l'objet.

XII. Entrée en vigueur

La présente charte est publiée par note de service, diffusée à l'ensemble des agents et accessible via l'Intranet institutionnel.

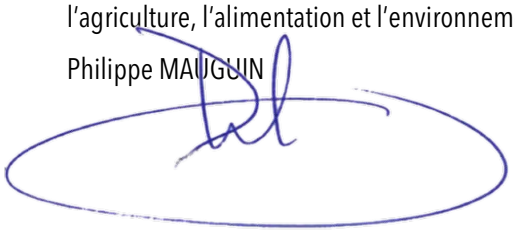
Elle abroge et remplace, à compter de la date de sa publication, toutes les dispositions contraires figurant dans les décisions ou notes de service antérieures.

Seule la version française de la présente charte est opposable.

Fait à Paris, le 01/01/2026

Le Président de l'Institut national de recherche pour l'agriculture, l'alimentation et l'environnement,

Philippe MAUGUIN



Annexe – Liens utiles

Cybersécurité

- Site intranet Cybersécurité : https://cybersecurite.intranet.inrae.fr
  - PGSSI et POSSI : https://intranet.inrae.fr/NS/ns2023-31.htm
  - Échelle de sensibilité de l'information : https://cybersecurite.intranet.inrae.fr/service-et-document/sensibilite-de-l-information-les-bons-reflexes/sensibilite-de-l-information
  - Instruction interministérielle 901 relative aux données sensibles non classifiées de défense : https://www.legifrance.gouv.fr/circulaire/id/39217
  - Instruction interministérielle 1300 relative aux données du secret de la défense nationale : https://cyber.gouv.fr/instruction-generale-interministerielle-n1300
  - Exemple de réseau sur lesquels la connexion d'un Matériel personnel est autorisée dans les conditions de la charte : Eduspot.
  - Guide des bonnes pratiques des Administrateurs de postes de travail : https://cybersecurite.intranet.inrae.fr/je-suis-informaticien/je-suis-gestionnaire-de-postes-de-travail/guide-metier-administrateurs
- Note de service n°2021-77 du 13/12/2021 relative aux contrôles des usages non conformes des Ressources Informatiques : https://intranet.inra.fr/NS/ns2021-77.htm
- Guide de départ de l'agent : https://systemes-information.intranet.inrae.fr/

Données personnelles

- Note de service n°2019-28 du 21/03/2019 relative aux modalités d'application de la réglementation relative à la protection des données à caractère personnel au sein de l'Institut **:** https://intranet.inrae.fr/NS/ns2019-28.htm
- Site intranet « Informatique et libertés - Données personnelles » : https://donnees-personnelles.intranet.inrae.fr/
  - Politique de Protection des Données personnelles d'INRAE : https://donnees-personnelles.intranet.inrae.fr/aspects-reglementaires-et-grands-principes/la-protection-des-donnees-a-inrae/politique-de-protection-des-donnees-a-caractere-personnelle-d-inrae
  - Information dédiée au traitement de ses données et l'exercice de ses droits : https://donnees-personnelles.intranet.inrae.fr/aspects-reglementaires-et-grands-principes/la-protection-des-donnees-a-inrae/vos-donnees-personnelles-a-inrae

Déconnexion

- Charte du droit à la déconnexion : https://ressources-humaines.intranet.inrae.fr/Media/Files/QVT/Dispositifs-existants/Charte-droit-deconnexion.

Empreinte environnementale du numérique

- Décret n°2024-134 d'application de l'article 58 de la loi 2020 AGEC : https://www.legifrance.gouv.fr/loda/id/JORFARTI000049184681/#JORFARTI000049184681
- Bonnes pratiques en matière d'envoi et de gestion des mails : https://librairie.ademe.fr/consommer-autrement/249-250-comment-teletravailler-leger-.htm

Communication

- Guide pour une communication responsable à INRAE : https://intranet.inrae.fr/national/vie-de-linstitut/le-guide-pour-une-communication-responsable-a-inrae-17410
- Charte d'expression publique, qui définit les principes à respecter lors de toute prise de parole ou publication à titre professionnel, afin de garantir la cohérence et la qualité des communications d'INRAE: https://intranet.inrae.fr/national/vie-de-linstitut/expression-publique-un-accompagnement-pour-tous-les-personnels-inrae-21526
- Charte graphique INRAE applicable aux communications et contenus d'INRAE : https://www.inrae.fr/sites/default/files/charte-graphique_inrae-avril-2024.pdf
- Règles typographiques en vigueur à INRAE : https://communication.intranet.inrae.fr/rubriques-verticales2/outils-de-communication/guide-typographique

Usage des ressources informatiques par les organisations syndicales

- Note de service n°2018-34 du 29/05/2018 relative aux conditions et modalités d'utilisation des technologies de l'information et de la communication par les organisations : https://intranet.inrae.fr/NS/ns2018-34.htm