



> S'INFORMER

Charte

INFORMATIQUE D'ONIRIS

Charte d'usage
du Système d'Information
d'Oniris VetAgroBio

La présente charte constitue le volet informatique du règlement intérieur d'Oniris VetAgroBio Nantes (ci-après Oniris).

Elle a été adoptée par son Conseil d'administration d'Oniris le 19 juin 2025 et devient opposable dès sa publication. Elle pourra être révisée en fonction de l'évolution des besoins, des technologies, et du cadre législatif et réglementaire.

Toute infraction à la présente Charte peut faire l'objet de poursuites disciplinaires, pénales et/ou civiles, le cas échéant.

Oniris se réserve par ailleurs le droit de retirer à tout moment, et sans préavis, les autorisations d'accès si le comportement d'un utilisateur n'est plus compatible avec les règles énoncées dans la présente charte ou relève d'une infraction.

Chaque utilisateur est tenu de respecter l'ensemble des règles définies dans la présente charte ainsi que les consignes de référence applicables publiées sur l'Intranet de l'établissement.

1 PORTÉE ET RESPONSABILITÉ

Cette charte est opposable à tous les utilisateurs de l'établissement, qu'ils soient notamment agents, personnels extérieurs hébergés, vacataires, invités, usagers extérieurs, étudiants ou stagiaires de la formation continue à l'école.

Elle est disponible sur l'intranet de l'école.

Cette Charte définit les règles d'utilisation de l'ensemble des moyens informatiques et numériques, et plus généralement du système d'information de l'établissement, les droits et devoirs des utilisateurs, les règles applicables sur la sécurité des données, les sanctions en cas de non-respect de ces règles et les procédures à suivre en cas d'incident.

A titre liminaire, il convient de relever que l'établissement met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection de l'utilisateur et, notamment, de ses données personnelles conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil 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.

L'utilisateur est responsable, en tout lieu et en tout temps, de l'usage qu'il fait du système d'information auquel il a accès.

2 DIFFÉRENTS USAGES DE RESSOURCES

PRINCIPES GÉNÉRAUX :

L'utilisation des ressources du système d'information d'Oniris est soumise à autorisation préalable. Cette autorisation est concrétisée par l'ouverture d'un à plusieurs comptes par une personne habilitée.

Ces comptes sont strictement personnels et inaccessibles, même temporairement, à un tiers. Les autorisations accordées sont susceptibles d'être retirées sans préavis si la qualité de

l'utilisateur ne le justifie plus ou en cas d'usage non conforme à la présente Charte. Chaque utilisateur a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède, conformément aux règles statutaires ou contractuelles qui lui sont opposables.

USAGE PROFESSIONNEL DES SERVICES ET DES RESSOURCES :

AU SEIN DE L'ÉCOLE :

Les ressources du système d'information ne doivent être utilisées que dans le cadre d'activités conformes aux missions de l'école et dans le respect du droit en vigueur.

L'ensemble du système d'information (utilisation des ressources informatiques, usage des services Internet, usage du réseau, etc.) est destiné à l'activité professionnelle telle que définie par les textes spécifiant les missions du service public de l'enseignement supérieur et de la recherche (*article L. 123-3 du Code de l'éducation et article L. 812-1 du Code rural et de la pêche maritime*).

A L'EXTÉRIEUR :

L'accès à distance à une partie du système d'information, notamment dans le cadre du télétravail, est autorisé par l'intermédiaire de dispositifs d'accès sécurisés.

Dans le cadre du travail à distance, l'ensemble des dispositions de ce document s'applique pleinement, tout comme la note de service ministérielle en date du 5 mai 2022 visée dans les textes de référence.

En outre, l'accès distant via le réseau privé virtuel (VPN) de l'établissement n'est autorisé qu'à partir d'équipements de l'établissement répondant aux pré-requis de sécurité.

Les utilisateurs auxquels sont attribués des équipements mobiles (ordinateur portable, téléphone portable, tablette) doivent apporter une attention toute particulière aux mesures de sécurité destinées à préserver l'intégrité de ces matériels et des données qu'ils contiennent, en particulier lorsqu'ils se trouvent à l'extérieur de l'établissement (en télétravail, dans les transports, à l'étranger...).

En cas de perte ou de vol d'un équipement ou de données, il est de la responsabilité de l'utilisateur de signaler sans délai l'incident à la DSI (conformément à la procédure disponible sur l'intranet.)

USAGE PRIVÉ DES SERVICES ET DES RESSOURCES :

L'utilisation du système d'information à titre privé est tolérée, à condition que celle-ci soit non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. Elle ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre, au bon fonctionnement du service et ne doit en aucun cas porter atteinte au fonctionnement et à l'image de l'établissement. Ces règles sont identiques pour l'usage des téléphones fixes ou mobiles (professionnels).

Toute utilisation du système d'information à des fins contraires à l'ordre public et aux bonnes mœurs est illégale et pourra faire l'objet de poursuites.

Toute information est réputée professionnelle et est consultable dans l'intérêt du service par l'autorité hiérarchique de l'utilisateur, à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée (sauf en présence et sur accord de l'utilisateur ou sur réquisition judiciaire ou administrative).

Ainsi, il appartient à chaque utilisateur de procéder au stockage de ses données à caractère privé dans un espace prévu explicitement à cet effet ou en mentionnant le caractère privé d'une partie

de ses données et en adoptant, exclusivement, les termes « privé », « prive », « personnel », « perso » ou « confidentiel », pour nommer le dossier ou l'objet du message contenant ces informations dans le respect du secret des correspondances privées (*article 432-9 modifié du Code pénal*).

La sauvegarde régulière des données à caractère privé incombe à l'utilisateur et se fait sous sa seule responsabilité.

GESTION DES ABSENCES OU DU DÉPART DE L'AGENT

En cas d'absence ou de départ de l'établissement et afin de répondre à l'obligation de loyauté et au principe de continuité du service public, ce dernier est tenu de communiquer, à son supérieur hiérarchique, les données et informations nécessaires à la poursuite de l'activité de l'école. Par contre, l'identifiant et les mots de passe restent confidentiels et ne peuvent pas être divulgués.

En cas d'impossibilité ou de refus de la part de l'utilisateur, Oniris peut prendre les mesures nécessaires pour accéder aux données professionnelles contenues sur les ressources informatiques de l'intéressé. Ces opérations ne peuvent s'opérer que sur demande du supérieur hiérarchique et après accord de la direction générale.

Préalablement à son départ, il appartient à l'utilisateur de remettre à la DSI l'ensemble des moyens matériels et logiciels mis à sa disposition dans un état permettant sa réexploitation.

L'utilisateur qui ne restituerait pas son matériel (ordinateur, téléphone...) dans un délai raisonnable après son départ pourra engager sa responsabilité pénale pour abus de confiance, lequel est sanctionnable de 5 ans d'emprisonnement et 375 000 euros d'amende (*article 314-1 du Code pénal*).

Une plainte sera systématiquement déposée par l'école.

Des demandes de réactivation temporaire d'un compte ou de dérogation à une suppression de compte peuvent être adressées à la DSI (demande hiérarchique motivée et formulée par écrit exclusivement sur le Portail Informatique de la DSI).

L'utilisateur est responsable de ses données à caractère privé. Lors de son départ définitif du service ou de l'établissement, il lui appartient de sauvegarder, le cas échéant, puis de détruire son espace de données à caractère privé ; la responsabilité de l'établissement ne pouvant être engagée quant à la conservation de cet espace personnel. En tout état de cause, les données non identifiées comme personnelles seront présumées professionnelles.

GESTION DES OBJETS CONNECTÉS

Les objets connectés personnels peuvent être utilisés uniquement sur des réseaux Wi-Fi dédiés et isolés fournis par l'établissement, à condition de respecter les consignes de sécurité disponibles sur l'intranet. Tout branchement physique à un équipement d'Oniris reste interdit.

L'usage, par les étudiants, des objets connectés, devra se faire en conformité avec les règlements des études et les prescriptions de l'administration de la scolarité.

3. USAGES SPÉCIFIQUES :

L'accès, via le système d'information Oniris, à d'autres réseaux professionnels est principalement fourni par le groupement d'intérêt public GIP RENATER (Réseau national de télécommunications pour la technologie, l'enseignement et la recherche). Afin de préserver le bon fonctionnement de ce réseau, l'utilisateur du système d'information Oniris est également soumis à la charte de bon usage de l'informatique et du réseau RENATER.

Les organisations syndicales représentatives utilisent les outils informatiques qui leur sont attribués

pour l'exercice de leur mandat syndical. L'utilisation de ces outils se fait sans contrôle des données, à l'exception du paramétrage initial desdits outils ou à une intervention dans le cas d'une crise cyber. Les étudiants bénéficient de droits d'accès limités et spécifiques au cadre pédagogique. Toute infraction, comme l'utilisation des ressources pour le téléchargement illégal ou des usages non conformes à la mission éducative, pourra entraîner une suspension des accès et, le cas échéant des sanctions.

4. MÉDIAS ET OBLIGATIONS DÉONTOLOGIQUES

Dans son usage privé d'internet, l'utilisateur ne doit jamais utiliser d'identifiants et de mots de passe similaires à ceux utilisés pour accéder aux ressources de l'établissement. Le cas échéant, l'établissement se réserve le droit d'effectuer tout changement sur le compte Oniris utilisateur concerné, après en avoir informé l'intéressé.

Sur internet (réseaux sociaux par exemple), lorsque l'utilisateur s'exprime à titre privé, il ne doit pas utiliser son adresse email professionnelle.

Il peut mentionner son appartenance à l'établissement sur des réseaux sociaux à vocation professionnelle mais en veillant à ne jamais divulguer d'informations confidentielles ni à entacher l'image de l'administration d'une quelconque façon. Il en est de même pour les réseaux sociaux à usage personnel ou récréatif et une très grande prudence est demandée aux utilisateur.

En tout état de cause, tout agent reste tenu dans ce cadre par ses obligations de neutralité et de réserve y compris en dehors de son temps de travail. S'il est usager du service public, il s'expose à des poursuites disciplinaires en cas de manquement à ses obligations déontologiques.

L'étudiant est responsable de l'information qu'il communique sur les médias sociaux tels que les forums, les blogs, les réseaux sociaux, etc. Il respectera son devoir de réserve lorsqu'il s'exprimera sur ces médias. Le cas échéant porter atteinte à l'image de l'école expose l'étudiants à des poursuites disciplinaires.

Les personnels ayant pour mission de représenter officiellement l'établissement sur des réseaux sociaux doivent être nommément désignées et autorisées à communiquer ou publier par la Direction Générale de l'établissement.

5 PROTECTION DES PROPRIÉTÉS INTELLECTUELLES ET DES DONNÉES PERSONNELLES

PROPRIÉTÉS INTELLECTUELLES

L'utilisation du système d'information de l'établissement implique le respect des droits de propriété intellectuelle tels que définis dans le Code de la propriété intellectuelle et du droit à l'image (article 9 du Code civil).

Sans que cette liste soit exhaustive, l'utilisateur s'engage à :

- ✓ Utiliser les logiciels et applications, dans les conditions de la licence souscrite par l'établissement ;
- ✓ Ne pas effectuer de copie illicite de logiciel ou d'applications et, a fortiori, de tenter d'installer des logiciels ou applications pour lesquels l'établissement ne posséderait pas un droit d'usage ;
- ✓ Ne pas reproduire, copier, utiliser remettre à des tiers ou diffuser, les bases de données, pages web, dessins, modèles, logos ou autres créations de l'établissement ou de tiers protégés par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;

- ✓ *Ne pas reproduire, copier ou diffuser des textes, des images, des photographies, des œuvres musicales, audiovisuelles ou multimédia et, plus généralement, toute création ou invention provenant du réseau internet, d'applications web ou mobiles, sans autorisation ou licence ;*
 - ✓ *Ne pas reproduire, copier, utiliser ou diffuser des éléments susceptibles de porter atteinte à l'image ou à la vie privée des utilisateurs ou de tiers à l'établissement.*
- Chaque étudiant, quel que soit son cycle d'étude, s'engage à respecter la Charte anti plagiat de l'école.*

PROTECTION DES DONNÉES PERSONNELLES

Les utilisateurs sont informés de la nécessité de respecter la réglementation en matière de traitements 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.

Les données à caractère personnel sont des informations qui permettent - sous quelque forme que ce soit - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Selon le RGPD :

Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.

Le principe de finalité limite la manière dont vous pourrez utiliser ou réutiliser ces données dans le futur et évite la collecte de données « au cas où ».

Le principe de minimisation limite la collecte aux seules données strictement nécessaires à la réalisation de votre objectif.

Aussi tout agent ou tout étudiant qui souhaite collecter des données personnelles, quelle qu'en soit la finalité, doit s'adresser au D.P.O. de l'école, en charge de la tenue du registre des traitements d'Oniris en écrivant à : contact.dpd@oniris-nantes.fr

ou

**Le Délégué à la protection des données personnelles d'Oniris VetAgroBio Nantes
Oniris VetAgroBio Nantes
101 route de Gachet
44300 Nantes.**

6 SÉCURITÉ

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 utilisateur et de manière générale tout dysfonctionnement ;*
- ✓ *Ne jamais confier son identifiant/mot de passe à un tiers ;*
- ✓ *Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur ;*
- ✓ *Conserver de façon sécurisée ses mots de passe.*
- ✓ *Ne pas modifier et/ou contourner les paramètres de sécurité du poste de travail ;*

Verrouiller son ordinateur dès qu'il quitte son poste de travail ;

- ✓ Ne pas utiliser les services qui lui sont offerts pour proposer ou rendre accessibles à des tiers des données et informations confidentielles ou contraires à la législation en vigueur*
 - ✓ Ne pas installer, télécharger ou utiliser sur le matériel connecté au réseau d'Oniris des logiciels ou progiciels ou matériels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de la DSI ;*
 - ✓ Ne pas modifier la configuration des ressources (matériels, réseaux, branchements...) mises à sa disposition, sans avoir reçu l'accord et l'aide préalables des personnes habilitées de la DSI ou d'un correspondant informatique.*
 - ✓ Ne pas déposer des données sur un serveur interne ou ouvert au grand public sans y être autorisé*
 - ✓ Se conformer aux dispositifs mis en place par Oniris pour lutter contre les virus et les attaques*
 - ✓ Ne pas connecter au réseau filaire de l'établissement des équipements externes ou tout autre matériel non préalablement autorisé par la DSI. La connexion d'équipements externes n'est autorisée que sur les réseaux Wi-Fi dédiés à cet usage.*
 - ✓ Ne pas se connecter à Internet via un équipement (routeur 4G/5G) non maîtrisé par la DSI*
Dans tous les cas, pour accéder aux réseaux filaires et Wi-Fi, l'utilisateur doit être identifié avec le compte nominatif qui lui aura été attribué.
- L'établissement se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.*

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formation ou de campagnes de sensibilisation, certaines pouvant être rendues obligatoires.

Il est également informé que pour effectuer la maintenance corrective, curative ou évolutive, l'établissement se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition

L'établissement organise des sessions de formation obligatoires tous les semestres pour sensibiliser les utilisateurs aux règles de sécurité informatique, notamment sur les risques liés au hameçonnage, aux mots de passe faibles et à l'utilisation des réseaux non sécurisés. Des supports pédagogiques seront également disponibles sur l'intranet.

7 CHARTRE DES ADMINISTRATEURS

La charte des administrateurs systèmes, réseaux et systèmes d'information est destinée à préciser les devoirs et les droits de toutes personnes chargées de la gestion de ressources informatiques, de télécommunication ou logicielles.

DROITS DES ADMINISTRATEURS

Seuls les administrateurs jouissent de droits d'accès étendus sur le système d'information. Les droits de l'administrateur sont liés aux missions exercées en lien avec sa fiche de poste et sur son périmètre de responsabilité strict. Les droits de l'administrateur ne sont pas liés à sa position hiérarchique.

L'administrateur doit avoir accès aux ressources, outils et formations nécessaires pour

exercer ses missions efficacement.

L'administrateur a le devoir de ne pas user de ses droits pour d'autres actions que celles légitimées par ses missions. Il ne doit en aucun cas nourrir son intérêt personnel au travers des actions qui lui sont permises et des accès à des informations confidentielles, personnelles le concernant ou concernant un tiers, sous peine de sanctions.

Tout particulièrement :

L'accès à distance à un ordinateur d'un utilisateur doit être réalisé avec le consentement préalable de l'utilisateur.

L'utilisation du mot de passe d'un tiers pour réaliser une quelconque opération sur le SI est formellement interdite. L'administrateur veillera, au contraire, après identification de toute utilisation non conforme d'un mot de passe, à imposer à l'utilisateur un changement de mot de passe dans les meilleurs délais ;

Les administrateurs doivent utiliser des outils de chiffrement fiables pour sécuriser les mots de passe qui leur sont confiés.

Il peut interdire tout flux informatique ainsi que tout équipement informatique, audiovisuel ou téléphonique présentant des risques pour la sécurité ou le bon fonctionnement du SI ou en infraction avec la présente charte. Il peut procéder à toute recherche préventive de faille sur les équipements informatiques ou téléphoniques, privés ou non, raccordés aux systèmes d'information.

En cas de compromission d'un équipement informatique, audiovisuel ou téléphonique, présentant un risque majeur avéré pour le fonctionnement ou la sécurité du SI, l'administrateur pourra reconfigurer ce matériel dans un état « sortie usine », au détriment des données stockées sur l'équipement qui seront détruites lors du processus. L'utilisateur reconnaît le droit à l'administrateur de réaliser cette opération dans un délai conciliant les impératifs de sécurité et la préservation des données de l'utilisateur.

DEVOIR DES ADMINISTRATEURS

L'administrateur doit se conformer strictement aux réglementations nationales, européennes et internationales relatives à la cyber sécurité, à la protection des données et à la propriété intellectuelle.

L'administrateur doit veiller à la protection des informations sensibles (notamment les données personnelles, données issues de la recherche, base de données comprenant des données personnelles ou cliniques...) de l'établissement et des utilisateurs contre tout accès non autorisé, divulgation, modification, suppression ou destruction.

Il doit veiller à identifier et conduire les actions de prévention permettant d'éviter toute altération illégitime du système d'information, et alerter toute personne compétente (DSI, délégué à la protection des données, CNIL, autorité hiérarchique...) de tout risque en la matière.

L'administrateur doit mettre en œuvre et maintenir des mesures de sécurité robustes, incluant la bonne application des mises à jour de sécurité sur les différentes composantes du système d'information, ainsi que la bonne mise en œuvre et l'efficacité des outils de sécurité déployés pour protéger le SI (pare-feu, filtrage Web, anti-virus, chiffrement des secrets, etc.).

Il ne doit mettre en œuvre que des solutions validées par la DSI afin d'assurer leur compatibilité avec le SI de l'établissement.

L'administrateur doit respecter les règles déontologiques propres à tous les agents publics.

L'administrateur est soumis dans l'exercice de sa fonction à un devoir de discrétion et est tenu

au secret professionnel. Pour assurer le bon fonctionnement et la sécurité du SI, il peut procéder aux investigations nécessaires (recherche de traces informatiques, vérification des accès, audit technique d'un poste de travail, etc.). Pour répondre à une réquisition judiciaire, l'autorité hiérarchique pourra demander aux administrateurs de communiquer les informations obtenues dans l'exercice de leurs fonctions et entrant dans l'objet de la réquisition, conformément au Code de procédure pénale.

8 MISES À JOUR ET RÉVISIONS

Cette charte sera mise à jour régulièrement, pour garantir sa conformité aux évolutions législatives et réglementaires.

Textes applicables

Code général de la fonction publique (CGFP), et notamment son livre premier ;

- *Code pénal ;*
- *Code rural et de la pêche maritime (CRPM) ;*
- *Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés;*
- *Règlement (UE) 2016/679 du Parlement européen et du Conseil 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, dit « RGDP ») ;*
- *Guides et notes techniques de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) : <https://www.ssi.gouv.fr/administration/bonnes-pratiques> ;*
- *Documents de la Commission nationale de l'informatique et des libertés (CNIL) : <https://www.cnil.fr/fr/travail-et-donnees-personnelles> ;*
- *Charte des temps du ministère chargé de l'agriculture (note de service SG/SRH/SDDPRS/2016-206 du 04/03/2015).*
- *Note de service du ministère chargé de l'agriculture sur les modalités pratiques de mise en œuvre du télétravail au ministère de l'agriculture et de l'alimentation (SG/SRH/SDDPRS/2022-363 du 05-05-2022)*
- *Circulaire de la Première ministre en date du 31 mai 2023 n°6404/SG relative à l'actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre »)*



Oniris
VetAgroBio Nantes
ÉCOLE NATIONALE

Campus Vétérinaire
101 Route de Gachet
CS 40706
44307 NANTES Cedex 3
02 40 68 77 77

www.oniris-nantes.fr



Campus Ingénieur
Rue de la Géraudière
CS 82225
44322 NANTES Cedex 3
02 51 78 54 54