

ANNEXE 4 : CHARTE INFORMATIQUE

(validé au CA du 12 mars 2026 – annexe du règlement intérieur)

1. Préambule

Le présent document définit les règles d'usage qui s'imposent à tout·e utilisateur·trice des matériels, systèmes, logiciels ou réseaux informatiques (désignés ci-après par ressources ou services numériques) de l'Institut National des Sciences Appliquées de Toulouse (INSA). Est utilisateur·trice toute personne qui fait usage des ressources ou services numériques de l'INSA (étudiant·e·s, personnels, personnels hébergés, collaborateur·trice·s bénévoles, etc.).

Cette charte précise les droits, devoirs et obligations des utilisateur·trice·s afin de garantir un usage correct et loyal des moyens informatiques, dans le respect des lois et d'autrui.

Cette Charte est annexée au Règlement Intérieur de l'INSA et en constitue un élément indissociable. Cette Charte entre en vigueur à compter du 12 mars 2026 et abroge tous les autres documents ou chartes relatifs à l'utilisation du système informatique de l'INSA.

L'INSA pourra faire évoluer cette Charte afin de se conformer aux évolutions légales, réglementaires, jurisprudentielles ; aux évolutions liées à l'usage des moyens informatiques ; ou pour toute autre raison qu'il juge pertinente. En cas d'évolution de cette Charte, l'INSA précisera la date d'entrée en vigueur des versions ultérieures.

2. Engagement de l'INSA de Toulouse

Le Centre des Services Numériques (CSN) de l'INSA, dans la mesure de ses possibilités et des contraintes qui lui sont imposées :

- Met à disposition des utilisateur·trice·s les matériels et les logiciels les plus adaptés à leurs besoins ;
- Fournit un accès au réseau de l'INSA et au travers de celui-ci à Internet via un compte informatique et éventuellement une adresse électronique ;
- Maintient et sécurise au mieux le parc informatique, le réseau et les données ;
- Assure la continuité du service offert.

Des périodes de maintenance obligatoires seront programmées par le CSN pour permettre la mise à jour des services numériques entraînant des perturbations sur ces services. Les utilisateur·trice·s seront informés en amont de ces maintenances.

3. Devoirs des utilisateur·trice·s

• Compte informatique

Le CSN met à disposition de chaque utilisateur·trice des ressources et services numériques un compte informatique sous la forme d'un identifiant et d'un mot de passe permettant d'y accéder. Cet identifiant est strictement personnel et inaccessible quel que soit le contexte. Il ne doit en aucun cas être réutilisé sur un service numérique autre que ceux fournis par l'INSA.

L'utilisateur·trice est responsable de la sécurité de son compte, il·elle doit s'assurer de la robustesse et son mot de passe et doit procéder à son changement en cas de divulgation ou de fuite.

• Bonne utilisation des ressources

L'utilisation des ressources et services numériques (réseau filaire, Wifi, applications, services "cloud" gérés, postes mis à disposition par le CSN, ...) est réservée aux travaux liés à l'enseignement, à la recherche et au fonctionnement de l'INSA.

Toutefois, une utilisation à des fins extra-professionnel est tolérée si cet usage est raisonnable, mesuré et ne peut en cas se faire au détriment des tâches ou missions « professionnelles ». Il ne doit en aucun cas nuire au bon fonctionnement de l'ensemble des ressources numériques de l'INSA ou altérer son image. En toute hypothèse, le surcoût qui résulte de l'utilisation privée résiduelle des systèmes d'information doit demeurer négligeable au regard du coût global d'exploitation.

- **Respect des règles légales et de sécurité**

Tout·e utilisateur·trice des ressources et services numériques se doit de respecter la législation en vigueur relative à l'utilisation des technologies de l'information et de la communication dont notamment celle applicable concernant :

- L'atteinte à la vie privée.
- Les propos contraires aux règles éthiques (diffamation, injures).
- La fraude informatique.
- La tentative d'accès ou maintien frauduleux dans un système de traitement de données,
- La violation de la propriété intellectuelle et du droit à l'image.

L'utilisateur·trice doit adopter un comportement responsable, raisonnable et agir en veillant notamment à la protection de son poste de travail et des services numériques de l'INSA. Il ne passe pas outre des avertissements ou fonctions de sécurité. En cas de doute, il prend conseil auprès du CSN avant d'effectuer toute opération.

L'ouverture de documents, liens, applications provenant de sources inconnues (mail, clés USB) doivent par exemple faire l'objet d'attentions particulières.

La saisie d'identifiants INSA (nom d'utilisateur·trice, mot de passe) depuis des périphériques non fiables (cybercafés), ou sur des sites non affiliés à l'INSA ou à apparence ou destination douteuse est interdit.

L'utilisateur·trice des ressources et services numériques doit également se conformer aux consignes du CSN (par exemple : mise à jour de l'antivirus et du système) et doit signaler tout incident, toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement. Il·elle est tenu·e de respecter le matériel de l'INSA et de ne pas modifier sa configuration (systèmes et logiciels) sauf accord préalable du CSN.

- **Matériel**

Le matériel confié (ordinateur, écrans, smartphone, périphérique externe, etc.) pour l'exercice des fonctions reste la propriété de l'INSA et devra être restitué au départ de l'utilisateur·trice, conformément au circuit de départ en vigueur. Il est de la responsabilité de l'utilisateur·trice de supprimer toutes ses données « privées » avant de restituer son matériel. A compter de la restitution du matériel, l'ensemble des données figurant sur celui-ci est présumé intégralement professionnel.

L'utilisateur·trice est responsable de son matériel, il se doit d'en prendre soin et d'être particulièrement vigilant en cas de déplacement hors du lieu de travail.

Lorsqu'un·e utilisateur·trice part en mission en l'étranger, selon le pays il·elle peut être amené à ne pas utiliser son poste personnel mais plutôt un poste vierge de données. L'utilisateur·trice doit suivre les recommandations de l'INSA en la matière. Si l'utilisateur·trice a des doutes sur sa destination, il doit se rapprocher du CSN.

- **Hygiène Numérique**

L'utilisateur·trice veille à la maintenance de son poste de travail. Il·elle s'assure qu'il reste à jour et sécurisé en planifiant rapidement les opérations demandées par les applications ou le CSN.

L'utilisateur·trice est également responsable des documents sur lesquels il·elle opère : il·elle doit s'assurer que leur accès est bien réservé aux personnes en ayant besoin, mis, classifiés et sauvegardés dans des espaces

communs si ces documents concernent l'activité de l'INSA.

De plus, dans un souci de réduction de l'emprunte numérique de l'INSA, l'utilisateur·trice fait une attention particulière aux données obsolètes et au stockage de données à caractère privé (ne relevant pas de l'activité de l'INSA), qui doit rester minime. Ces données sont supprimées ou classifiées dans un dossier nommé "privé" de l'espace de travail.

L'utilisateur·trice travaillant sur un PC non géré par le CSN (PC ou téléphone personnel ou fourni par un autre établissement) et amené à travailler sur des données professionnelles veille à limiter la rémanence de ces données et privilégie le stockage sur des ressources numériques fournies par l'INSA.

Chaque utilisateur·trice doit veiller à ce que son espace de travail physique ne donne pas accès à des données sensibles : ne pas afficher de mot de passe, ne pas laisser trainer des documents sensibles sur son bureau. Il·elle veille à fermer son espace de travail physique (dès que cela est possible) en cas d'absence.

4. Données des utilisateur·trice·s

Toutes les données (fichiers, courriels et publications notamment via le web) stockées sur des ressources ou services numériques de l'INSA ou produites dans le cadre de l'enseignement, de la recherche et du fonctionnement de l'INSA y compris sur un matériel n'appartenant pas à l'INSA (sur un service en mode SaaS), sont considérées, sauf mention contraire, à caractère professionnel et l'INSA en est le propriétaire.

En revanche, les données (fichiers, dossiers et courriels) avec la mention "PRIVE" ou "privé", ou toute autre mention équivalente traduisant la volonté claire de son titulaire d'en réserver l'accès, permettant raisonnablement d'identifier les données comme étant privées, sont considérées comme personnelles.

Quant aux publications sur Internet via les serveurs de l'INSA, elles sont par nature professionnelles.

Les données à caractère professionnel doivent être mises à disposition de la directrice de l'INSA pour les enseignant·e·s-chercheur·euse·s, ou du·de la responsable hiérarchique pour les autres utilisateur·trice·s, qui quittent l'INSA. À défaut, elles seront transmises par un·e administrateur·trice du CSN sur simple demande du·de la responsable hiérarchique.

Les données des étudiant·e·s à caractère professionnel peuvent être mises à disposition de l'équipe enseignante par un administrateur du CSN sur simple demande pour assurer la continuité de la formation.

En cas de violation de ces règles ou mesures d'urgence afin de préserver les systèmes et les données, le CSN peut être amené à examiner le contenu de l'ensemble des fichiers de l'utilisateur·trice. Les administrateur·trice·s doivent toujours respecter la confidentialité des informations dont ils auraient pu prendre, volontairement ou non, connaissance.

• Données sensibles

Les données sont dites "sensibles" si elles sont liées à des contrats, brevets, ou à des informations stratégiques ou financières sur l'INSA. L'explicitation des données sensibles peut être retrouvée dans la classification des données spécifique à l'INSA. Les données contenant des informations à caractère personnel, c'est à dire informations qui permettent, sous quelque forme que ce soit, directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent sont aussi considérées aussi comme des données sensibles et doivent faire l'objet d'une déclaration de traitement auprès du DPO (contact-dpo@insa-toulouse.fr).

L'ensemble des opérations (création, modification, stockage, archivage) sur les données sensibles doit uniquement s'effectuer sur du matériel ou des services opérés et habilités pour cela par le CSN. La conservation de ce type de données sur un équipement ou service non habilité par le CSN est strictement interdite.

- **Sauvegarde**

L'ensemble des données des utilisateur·trice·s stockés sur les ressources ou services numériques sont sauvegardées, sans distinction de noms des répertoires, fichiers ou messages (y compris ceux marqués privé) de façon à garantir la disponibilité en cas d'incident. Sur les postes nomades (ordinateurs portable), seul le dossier "NoBackup" n'est pas sauvegardé pour que l'utilisateur·trice puisse y déposer des documents qu'il ne souhaite pas sauvegarder.

- **Conservation**

Au départ de l'utilisateur·trice, les données produites par cet·te utilisateur·trice et stockées dans son répertoire de travail (homedir), ainsi que les messages électroniques sont conservés deux ans après la clôture du compte avant d'être supprimées. Les données stockées sur des espaces communs ou boîtes partagées sont conservées car de nature nécessaire à la continuité de l'activité.

- **Messagerie électronique**

L'utilisateur·trice·s voit attribuer une ou plusieurs adresse(s) électronique(s) institutionnelle lors de son arrivée à l'INSA lorsque cela s'avère nécessaire pour l'exercice des missions et pour un usage professionnel. Ces adresses peuvent être automatiquement abonnées à des listes de diffusions institutionnelles sans que les utilisateur·trice·s ne puissent s'y opposer.

Cependant, un usage raisonnable et ponctuel de la messagerie électronique dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que l'utilisation du courrier électronique n'affecte pas le trafic normal des messages institutionnels. Tous les courriels, reçus ou sauvegardés depuis les ressources et services numériques de l'université sont présumés être professionnel, à défaut d'avoir été clairement identifiés comme « PRIVE » ou « privé » par l'utilisateur·trice.

S'il reçoit par erreur un message dont il·elle n'aurait pas dû être destinataire, toute utilisation, copie ou diffusion, même partielle de ce message est interdite. Il·elle a l'obligation de le détruire et d'en informer immédiatement son expéditeur.

Les utilisateur·trice·s sont fortement invités à n'utiliser que les outils mis en œuvre par l'INSA pour la consultation et l'envoi des courriers électroniques (par exemple le webmail) ; il est fortement déconseillé de rediriger son courrier vers des serveurs externes.

Les échanges par courriers électroniques sur les serveurs de l'INSA font l'objet de mesures de sécurisation (antispam, antivirus, limitation sur les types et la tailles des pièces joints, vérification des expéditeurs avec des adresses institutionnelles).

En cas d'atteinte à la sécurité des données, le CSN peut prendre des mesures conservatoires nécessaires sur les boîtes de messagerie (suppression de messages).

5. Mesures de sécurité

L'INSA a mis en place des mesures techniques afin de surveiller, auditer et sécuriser des ressources et services numériques. Le CSN est susceptible de mener des actions ou mettre en place des mesures (suspension des accès au réseau) en cas de détection de comportement suspect de la part d'un·e utilisateur·trice ou d'un équipement numérique

Toute action visant à contourner ou tenter de contourner ces mesures est strictement interdite.

- **Accès Internet**

L'utilisation d'Internet n'est autorisée que dans le cadre d'un usage professionnel (administratif ou pédagogique).

Un filtrage a été mise en place sur l'accès Internet avant de préserver les ressources et services numériques de contenus malveillants et présentant un risque pour ces ressources.

Toutefois, un usage raisonnable des services de l'Internet est toléré dans le cadre privé, à condition que son utilisation n'affecte pas les performances des services numériques de l'INSA.

Les contenus en ligne susceptibles d'entraîner une consommation importante des ressources Internet peuvent également être réglementés.

Le réseau de l'INSA étant raccordé à Internet via le réseau national Renater, les utilisateur·trice·s doivent également se conformer à la charte Renater qu'ils soient connectés en filaire ou en WIFI :

<https://www.renater.fr/wp-content/uploads/2022/01/charte-de-bon-usage-de-linformatique-et-du-reseau-renater.pdf>

<https://www.renater.fr/wp-content/uploads/2022/01/charte-deontologique-renater-fr.pdf>

6. Départ

Lors du départ d'un·e utilisateur·trice, celui·celle-ci doit supprimer ses données privées de son poste de travail, de ses espaces de stockage partagé. Il·elle doit rendre l'ensemble du matériel en sa possession au CSN y compris celui fourni dans le cadre du télétravail.

Il lui est recommandé de se désabonner des listes et de signaler son départ aux services / départements / laboratoires et centres avec lesquels il·elle est en interaction.

7. Traçabilité

Pour des nécessités d'investigation judiciaire, de sécurité, de maintenance et de gestion technique, les données de connexion, permettant d'identifier le poste ou l'utilisateur·trices sont conservées ainsi que l'historique de l'activité pendant le délai recommandé par la Commission Nationale de l'Informatique et des Libertés. Cela peut concerner les volumes échangés, l'identification des sites web consultés, la circulation des courriels, sans toutefois retranscrire les contenus.

8. Sanctions

En cas de non-respect des principes édictés précédemment, les utilisateur·trice·s concerné·e·s pourront se voir interdire provisoirement par le CSN l'accès aux ressources informatiques après débat contradictoire ou en cas de force majeure. Ils pourront faire appel de cette décision auprès de la directrice de l'INSA.

Les sanctions relevant de la procédure disciplinaire dans les établissements d'enseignement supérieur sont applicables.

Les sanctions civiles et pénales telles que prévues par les lois en vigueur sont également applicables.