INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

Version Octobre 2023

Charte informatique pour les utilisateurs de l'INSA Lyon

1. Préambule

La présente charte a pour objet de fixer les règles d'usage des moyens numériques de l'INSA Lyon.

Par « établissement » l'on entend l'INSA Lyon.

Par « système d'information » (SI), l'on entend l'ensemble des moyens mis en œuvre par l'établissement pour opérer les services nécessaires à ses missions et qui traitent les informations de gestion, d'enseignement et de recherche.

Par « moyens numériques », l'on entend tous les éléments et toutes les ressources constituant le système d'information (SI) de l'établissement. Les moyens numériques représentent ainsi l'ensemble des logiciels et services numériques que l'établissement met à disposition de ses utilisateurs. Cela inclut également les matériels informatiques, les logiciels, les données, les personnes, les infrastructures, le réseau.

Par « utilisateur » l'on entend l'ensemble des personnes ayant obtenu l'autorisation d'accéder au système d'information de l'établissement, dans le cadre de l'exercice de leur activité professionnelle ou pédagogique.

Par « données personnelles », l'on entend toutes les informations permettant d'identifier des personnes physiques de manière directe ou indirecte.

Par dossier personnel « Home », l'on entend un répertoire sur un serveur centralisé auquel seul l'utilisateur a des droits d'accès en lecture et en écriture. Et également, pour les personnels ayant accès à la plateforme de travail collaboratif GoFast, leur espace personnel de stockage sur celle-ci.

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à tous les métiers de l'établissement, à tous ses sites et locaux, à tous les utilisateurs de son SI, y compris les étudiants, stagiaires, auditeurs, à tous les supports de l'information et à tous les types d'accès.

Le bon fonctionnement du système d'information suppose par ailleurs le respect des dispositions législatives et réglementaires qui s'imposent, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

Les utilisateurs ayant des fonctions d'administrateur des moyens numériques sont soumis à une charte complémentaire et spécifique précisant leurs obligations particulières.

Les usages relevant de l'activité des organisations syndicales seront régis par un document spécifique qui viendra compléter la présente charte.

L'ensemble de ces documents est accessible en ligne et notamment sur l'intranet de l'établissement.

2. Conditions d'utilisation du système d'information et des moyens numériques

2.1 Utilisation professionnelle / privée

L'établissement met à la disposition de ses utilisateurs un ensemble d'outils et de services numériques à des fins professionnelles et pédagogiques.

Au sens de la présente charte, l'usage des moyens numériques présente un caractère professionnel lorsqu'il intervient :
- dans le cadre des missions confiées par l'établissement, pour les utilisateurs membres de son personnel : enseignants, personnels administratifs ou techniques, mais également ses prestataires et partenaires;
- dans le cadre des activités pédagogiques, pour ses utilisateurs étudiants.

Par opposition, l'utilisation des moyens numériques à des fins privées est tolérée lorsqu'elle n'entre pas dans

ce cadre professionnel. Cette utilisation privée doit être raisonnable, non-lucrative et limitée tant dans la fréquence que dans la durée. Elle ne doit nuire ni à la qualité du travail de l'utilisateur, ni au temps qu'il y consacre, ni au bon fonctionnement du service.

En toute hypothèse, le surcoût qui résulte de l'utilisation privée résiduelle des moyens numériques doit demeurer négligeable au regard du coût global d'exploitation.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées comme 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. Pour différencier les messages électroniques professionnels et personnels, l'utilisateur peut créer un sous-dossier spécifique dédié au contenu privé. 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.

Toute donnée présente sur un poste professionnel est réputée professionnelle, en ce sens que l'établissement pourra si nécessaire y accéder. Les dossiers identifiés comme personnels ou dont le caractère personnel est constaté ou déduit ne sont en principe pas accessibles.

L'établissement met également à disposition de l'utilisateur un dossier personnel privatif « Home » dans lequel il peut stocker des données personnelles et professionnelles.

2.2 Continuité de service : gestion des absences et des départs

Lors d'un départ définitif ou d'une absence ponctuelle, l'utilisateur informe sa hiérarchie des modalités d'accès aux applications et données permettant d'assurer la continuité de service.

En cas d'absence, les personnels s'engagent à mettre en place sur leur messagerie un message d'absence en réponse automatique indiquant les coordonnées d'une personne apte à prendre en charge les demandes urgentes qu'ils gèrent habituellement, ainsi que la date de leur retour.

Les mesures de conservation des données professionnelles sont définies avec le responsable hiérarchique désigné au sein de l'établissement.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou de l'établissement, l'utilisateur sera averti de la date de fermeture de son compte. Il lui appartient de supprimer ses données et détruire son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace.

3. Principes de sécurité

3.1 Règles de sécurité applicables

L'établissement met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs.

L'utilisateur est informé que les données stockées dans les espaces partagés ou son dossier personnel « home » mis à disposition par l'établissement sont sauvegardées régulièrement. L'utilisateur doit toujours privilégier les espaces partagés ou son dossier personnel « home » pour enregistrer ses données.

La sauvegarde des dossiers locaux du poste de travail, ou d'un périphérique externe, n'est pas prise en charge par l'établissement.
Les espaces partagés et le répertoire "Home" ne doivent pas être utilisés pour stocker de telles sauvegardes, ni des données volumineuses telles que des données de recherche.

L'utilisateur est informé que les mots de passe constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas un caractère personnel aux outils informatiques protégés.

Les niveaux d'accès ouverts à l'utilisateur sont définis en considération de la mission qui lui est confiée. La sécurité des ressources mis à sa disposition lui impose :
- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe (consultables sur https://dsi.insa-lyon.fr rubrique Catalogue de services->Conseil et Expertise->Sécurité Informatique->Mots de passe);
- de garder strictement confidentiels son ou ses mots de passe et ne pas les dévoiler à un tiers;
- de respecter la gestion des accès, en particulier ne pas utiliser l'identifiant et mot de passe d'un autre utilisateur, ni chercher à les connaître.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions:
De la part de l'établissement :
- veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées (en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie);
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.

De la part de l'utilisateur :
- si l'utilisateur ne bénéficie pas d'une habilitation explicite, il doit s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, même si cet accès est techniquement possible;
- ne pas installer, télécharger ou utiliser sur le matériel de l'établissement, des logiciels sans y être autorisé;
- se conformer aux dispositifs mis en place par l'établissement pour lutter contre les virus et les attaques informatiques.

3.2 Devoirs de signalement

L'utilisateur doit avertir la Direction des Systèmes d'Information (directeur.dsi@insa-lyon.fr) et le Responsable de la Sécurité des Systèmes d'Information (rssi@insa-lyon.fr) dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte, telle une intrusion dans le système d'information. Il doit signaler également à la personne responsable du service concerné toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

3.3 Mesures de contrôle de la sécurité

L'utilisateur est 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;
- qu'une prise en main à distance de son poste par un technicien de la DSI est précédée d'un avertissement;
-qu'il doit laisser se dérouler correctement les mises à jour automatiques effectuées sur son poste;
- que tout élément numérique considéré comme nuisible pour le système d'information pourra être supprimé automatiquement sans préavis de l'utilisateur, incluant notamment des programmes, fichiers, mails et pièces jointes.

L'établissement informe l'utilisateur que le système d'information peut faire l'objet d'une surveillance et d'un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

3.4 Protection des postes de travail : antivirus et chiffrement des supports de stockage

L'établissement a déployé une protection logicielle généralisée non seulement sur les serveurs mais aussi les postes de travail des utilisateurs. Le but d'un anti-virus est de protéger toutes les machines du parc contre les attaques provoquées par des codes malveillants. Sur chaque poste utilisateur est installé un client anti-virus. Il est interdit par la présente charte de désactiver, d'altérer le fonctionnement ou de désinstaller ce client. Il est aussi interdit d'utiliser d'autres logiciels (anti-virus ou autres) susceptibles d'entraîner un dysfonctionnement de l'antivirus installé en exécution de la stratégie de sécurité de l'établissement.

Les supports de stockage des postes de travail des laboratoires (pc fixes et ordinateurs portables) doivent obligatoirement être protégés par un mécanisme de chiffrement ("cryptage").
Les supports de stockage des ordinateurs portables des personnels administratifs (BIATSS) sont également protégés par ce mécanisme de chiffrement.

3.5 Utilisation du réseau

L'utilisateur s'engage à utiliser de façon raisonnable le réseau mis à sa disposition sur son poste et dans son service. Il ne doit pas effectuer d'opérations pouvant nuire au bon fonctionnement général du réseau de l'établissement, ce qui inclut notamment :
- Les transferts réseau occupant une partie trop importante de la bande passante disponible;
- L'utilisation de logiciels malveillants (attaques DOS, malwares...);
- L'utilisation de logiciels visant à rechercher ou exploiter des failles de sécurité dans le système d'information;
- La manipulation frauduleuse de la configuration réseau (usurpation d'adresse IP ou d'adresse MAC).

Il n'est pas autorisé à utiliser au sein de l'établissement un équipement réseau tel que hub, switch, routeur, borne wifi, etc., pouvant interférer avec l'infrastructure gérée par le CISR. En cas de besoin, l'utilisateur doit faire une demande de support par ticket à la DSI, qui transmettra au CISR, afin d'obtenir leur accord au préalable.

Par sécurité, l'utilisateur qui souhaite connecter sur le réseau filaire du matériel informatique personnel ou professionnel, qui n'est pas géré par la DSI ou par le service informatique de son entité, doit d'abord le déclarer auprès de la DSI, obtenir son accord et suivre la procédure associée.

4. Communications électroniques

4.1 Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'échange de l'information au sein de l'établissement.

La messagerie est un outil de travail destiné à des usages professionnels : elle peut néanmoins constituer le support d'une communication privée telle que définie à la section 2.1, dans la limite d'une utilisation raisonnable.

Adresses de messagerie électronique
L'établissement met à disposition de ses personnels et de ses étudiants une boîte de courrier électronique professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative, il ne retire en rien le caractère professionnel de la messagerie.

L'adresse électronique nominative est attribuée à un utilisateur qui la gère sous sa responsabilité.

Une adresse électronique fonctionnelle ou organisationnelle peut être mise en place si elle est exploitée par un service ou un groupe d'utilisateurs pour les besoins de l'établissement.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'utilisateurs, relève de la responsabilité exclusive de l'établissement : ces adresses ne peuvent être utilisées sans autorisation explicite.

L'utilisateur s'engage à limiter au maximum l'utilisation de sa messagerie électronique professionnelle pour des échanges relevant de sa vie privée et en dehors des activités liées à sa mission dans l'établissement.

Contenu des messages électroniques

Les messages électroniques permettent d'échanger principalement des informations à vocation professionnelle liées à l'activité de l'établissement ou au sein de l'établissement. En toutes circonstances, l'utilisateur doit adopter un comportement responsable et respectueux dans ses communications électroniques. Il s'interdit également de se faire passer pour une autre personne, d'envoyer un message anonyme ou de tenter de se substituer à une machine.

Sont notamment interdits les messages électroniques dont le contenu contrevient au droit d'auteur, propage des informations à caractère injurieux, raciste, xénophobe, sexiste, diffamatoire, harcelant, pornographique, obscène, ou portant atteinte à la vie privée ou à l'image d'autrui. Les auteurs de messages contenant de telles mentions sont susceptibles de faire l'objet de poursuites judiciaires et de poursuites disciplinaires par l'établissement.

Pour préserver le bon fonctionnement du service, une limitation du stockage des messages électroniques est mise en place pour tous les utilisateurs.

Émission et réception des messages électroniques
L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service. Des recommandations sont présentées dans le guide pratique de l'utilisateur.

Statut et valeur juridique des messages
Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat ou constituer une décision attributive de droits,. L'utilisateur doit en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

Stockage et archivage des messages
Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve. Le guide pratique de l'utilisateur présente un ensemble de règles impératives et des recommandations dont le respect garantit la conservation de ces données.

Transfert des messages vers une messagerie extérieure
Le transfert des messages vers une messagerie extérieure est interdit. En particulier, il est interdit de faire suivre automatiquement les messages vers une boîte mail personnelle (ex. : Gmail, hotmail...). Néanmoins, le transfert de message peut être toléré quand celui-ci est à destination d'une boîte mail d'une autre institution (ex. : CNRS, Inria...).
Cette fonctionnalité étant bloquée par défaut, l'utilisateur qui souhaiterait mettre en place une telle redirection professionnelle devra en faire la demande via un ticket de support à la DSI. La DSI mettra en place cette redirection après accord du RSSI.

4.2 Services numériques externalisés

Est considéré comme service externalisé tout service numérique dont la plateforme n'est pas hébergée ou gérée par l'établissement.

L'utilisation d'un service externalisé est soumise à l'application de la PSSIE (Politique de sécurité des systèmes d'informations de l'État) qui fixe les règles de protection applicables aux systèmes d'information de l'État. Chaque ministère est responsable de l'application de la PSSIE entrée en vigueur le 29 août 2014.

Avant toute utilisation d'un service externalisé non-approuvé par la DSI, les utilisateurs doivent s'assurer du niveau de conformité du service par rapport aux règles de la PSSIE, qui rappelle notamment « la nécessité pour les administrations de l'État de recourir à des produits et à des services qualifiés par l'ANSSI, ainsi qu'à un hébergement sur le territoire national de leurs données les plus sensibles ».

Les utilisateurs qui font transiter des données de l'établissement sans chiffrement sur un service externalisé non-approuvé par l'établissement engagent leur responsabilité. L'établissement décline toute responsabilité

en cas de survenance d'un incident.

4.3 Internet

Il est rappelé que le réseau Internet est soumis à l'ensemble des règles de droit en vigueur.

L'utilisation de la technologie Internet (et par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'établissement.

L'établissement met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible.

Internet est un outil de travail ouvert à des usages professionnels et pédagogiques : il peut constituer le support d'une communication privée telle que définie en section 2.1 dans le respect de la législation en vigueur.

Publications sur les sites web de l'établissement
Toute publication de pages d'information sur les sites internet ou intranet de l'établissement doit être validée par un responsable de site ou responsable de publication nommément désigné.

Sécurité
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 formations ou de campagnes de sensibilisation, relayées notamment via l'Intranet de l'établissement.

4.4 Téléchargements

Tout téléchargement de fichiers, notamment de vidéos, de musiques ou de logiciels, doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article 6.

L'établissement se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité du système d'information, tels les virus, codes malveillants ou programmes espions.

D'une façon générale, l'utilisateur doit restreindre ses téléchargements au cadre de son activité professionnelle.

5. Traçabilité

L'établissement est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées. Les dispositifs de traçabilité sur les outils et services numériques qu'il met à disposition des utilisateurs fait l'objet d'une déclaration préalable auprès de la Commission Nationale de l'Informatique et des Libertés.

6. Respect de la propriété intellectuelle

L'établissement rappelle que l'utilisation des moyens 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.
En conséquence, chaque utilisateur doit :
- Utiliser les logiciels dans les conditions des licences souscrites;
- S'abstenir de reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur, sans avoir obtenu

préalablement l'autorisation du ou des titulaires de ces droits.

Ressources documentaires numériques
La consultation des ressources documentaires électroniques mises à disposition implique de respecter les points suivants :
- L'usage de ces ressources par l'utilisateur doit se faire à titre professionnel, c'est à dire limité aux activités de l'administration, de la recherche et de l'enseignement dans le cadre des activités de l'établissement;
- L'utilisateur a le droit de visionner à l'écran et d'imprimer les ressources dans les limites d'un usage raisonnable, non commercial et strictement personnel;
- L'accès aux ressources est contrôlé et tout usage anormal détecté sera sanctionné (téléchargement massif, etc.);
- Toute rediffusion des ressources, même gratuite, est interdite.

7. Protection des données à caractère personnel

Le traitement des données à caractère personnel est effectué conformément au règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (RGPD) et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Les utilisateurs traitant des données à caractère personnel, dans le cadre de leurs attributions, et plus généralement dans le cadre de l'utilisation des outils informatiques, sont tenus de respecter la réglementation en vigueur. Ils s'engagent à protéger la confidentialité des informations auxquelles ils ont accès et à ne pas les transmettre à des personnes non expressément autorisées à les recevoir. Chaque utilisateur doit prendre les mesures nécessaires permettant d'éviter l'utilisation détournée des données traitées. Une fois qu'il quitte l'établissement, l'utilisateur s'engage à ne conserver aucune copie des données et de les restituer, dans leur intégralité, à l'INSA Lyon.

Le responsable de traitement est le Directeur de l'INSA Lyon.

Finalités des traitements
Les données sont collectées et traitées pour les finalités suivantes :
- Constituer un annuaire des comptes utilisateurs;
- Permettre un accès aux ressources informatiques mises à disposition sur les réseaux informatiques de l'établissement;
- Permettre un accès authentifié aux ressources et services informatiques mis en œuvre sur le réseau informatique de l'INSA Lyon;
- S'assurer du respect de la réglementation lors de la circulation des données sur Internet;
- Assurer le stockage et/ou de l'archivage de fichiers et des courriels des utilisateurs.

Types de données traitées
L'établissement traite toutes les données personnelles concernant les utilisateurs qui sont hébergées sur nos serveurs et provenant des services et entités de l'INSA Lyon.

Pour la navigation sur Internet, l'établissement traite les données sur le trafic (requête, IP source, identifiant, URL), ainsi que les cookies (témoins de connexion) qui peuvent mémoriser les actions et les préférences. L'INSA Lyon d'une politique relative aux cookies disponible sur notre site Internet.

Conservation et sécurité des données
Les durées de conservation des données à caractère personnel sont définies selon la réglementation en vigueur et conformément à la politique relative à la protection des données de l'établissement.

L'INSA Lyon met en œuvre toutes les mesures organisationnelles et techniques appropriées pour préserver la sécurité, l'intégrité et la confidentialité des données à caractère personnel et notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Si une faille de sécurité devait être constatée dans le traitement des données susceptibles d'entraîner un

risque élevé pour les droits et libertés, l'utilisateur concerné en sera informé conformément à la procédure en vigueur en cas de violations des données.

De même tout utilisateur est tenu de signaler à la DSI toute violation ou tentative de violation de son compte informatique.

Seront détaillées la nature de la violation rencontrée et les mesures mise en place pour y mettre un terme.

Exercice des droits
Chaque utilisateur dispose, pour des motifs réglementairement admis, des droits d'accès, de rectification, d'opposition, d'effacement, de portabilité et de limitation du traitement, relatifs à l'ensemble des informations le concernant.

Le droit d'accès ou de rectification des données personnelles est effectué sur simple demande. Leur effacement ou la limitation de leur traitement est conditionné par la réglementation en vigueur et dépend de la base légale du traitement.

À moins que la réglementation ne le permette pas, tout utilisateur peut, pour des motifs légitimes, s'opposer au traitement de ses données personnelles.

Il est également possible de récupérer les données personnelles (droit à la portabilité) quand celles-ci ont été recueillies sur la base d'un contrat ou du consentement de l'intéressé.

Pour exercer ces droits, il faut solliciter le Délégué à la Protection des Données personnelles qu'il est possible de contacter par courriel dpo@insa-lyon.fr

8. Limitations des usages

En cas de non-respect des règles définies dans la présente charte, le Directeur pourra, après en avoir averti l'intéressé et sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre de l'utilisateur, limiter les usages par mesure conservatoire :
- Limiter les accès de l'utilisateur;
- Déconnecter l'utilisateur, avec ou sans préavis selon la gravité de la situation;
- Retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes;
- Isoler, compresser ou effacer tout fichier trop lourd, ou manifestement en contradiction avec la charte, ou qui mettrait en péril la sécurité des ressources;
- Interdire à l'utilisateur tout accès aux ressources dont il est responsable.

9. Entrée en vigueur de la charte

La présente charte est annexée au règlement intérieur de l'INSA Lyon.

Le présent document annule et remplace toute version antérieure de la charte informatique, et s'ajoute à tout document ou chartes relatifs à l'utilisation des moyens numériques.

Le Directeur,

M. Frédéric FOTIADU

LE DIRECTEUR - INSA de Lyon -