CHARTE D'UTILISATION DES RESSOURCES INFORMATIQUES DE L'ENSAIT

Annexe 1.2 du règlement intérieur de l'ENSAIT

Table des matières

Préambule : 3
ARTICLE 1 – CHAMP D'APPLICATION 4
ARTICLE 2 – CONDITION D'UTILISATION DES SYSTEMES D'INFORMATION 4
2.1 Utilisation professionnelle / privée 4
2.2 Continuité de service : gestion des absences et des départs 4
ARTICLE 3 – PRINCIPES DE SECURITE 4
3.1 Règles de sécurité applicables 4
3.2 Devoirs de signalement et d'information 5
3.3 Mesures de contrôle de la sécurité 5
3.4 Avis de la Direction des Systèmes d'Information (DSI) avant l'acquisition de matériel informatique 6
ARTICLE 4 – COMMUNICATIONS ELECTRONIQUES 7
4.1 Messagerie électronique 7
4.2 Adresses électroniques 7
4.3 Contenu des messages électroniques 7
4.4 Statut et valeur juridique des messages 7
4.5 Internet 7
4.6 RENATER 8
4.7 Echange de fichiers 8
ARTICLE 5 – RESPECT DES DISPOSITION LEGALES SUR LA PROTECTION DES DONNES PERSONNELLES 8
ARTICLE 6 – LIMITATION DES USAGES 9

Préambule :

La présente charte définit les règles d'usages et de sécurité que l'Ecole Nationale Supérieure des Arts et Industries Textiles (ENSAIT) et l'utilisateur s'engagent à respecter. Elle précise les droits et devoirs de chacun.

Le bon fonctionnement du système d'information suppose 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.

Par « système d'information » (SI) s'entend l'ensemble des ressources matérielles et logicielles, fichiers applications, base de données et réseaux de télécommunication, pouvant être mis à disposition des utilisateurs par l'ENSAIT. L'informatique nomade (assistants personnels, ordinateurs portables, téléphones portables…etc.) est également un des éléments constitutifs du système d'information.

Par « utilisateur » s'entend toute personne autorisée à accéder aux ressources du système d'information dans le cadre de l'exercice de son activité à l'ENSAIT, quel que soit son statut.

Ainsi sont notamment désignés :

- Tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'enseignement supérieur et de la recherche.
- Tout étudiant inscrit à l'ENSAIT, y compris les apprentis.
- Tout prestataire ou partenaire ayant contracté avec l'ENSAIT.
- Tout personne autorisée à accéder à un service numérique de l'ENSAIT.

Engagement de l'ENSAIT

L'ENSAIT porte à la connaissance de l'utilisateur la présente charte et met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs. L'ENSAIT facilite l'accès des utilisateurs aux ressources du système d'information nécessaires.

Les ressources mises à leur disposition sont prioritairement à usage professionnelle, ou pédagogique, mais l'établissement est tenu de respecter la vie privée de chacun dans les conditions décrites ci-après.

Les personnels administrateurs du système d'information de l'ENSAIT sont soumis, dans le cadre de leurs missions, à des obligations inscrites dans la « *Charte informatique administrateurs* ». Les utilisateurs souhaitant être co-administrateur d'un ou de plusieurs postes informatiques sont également soumis à des obligations stipulées dans le « Contrat de co-admininistration ». Ces deux documents sont annexés au règlement intérieur de l'ENSAIT et disponibles sur l'intranet.

Engagement de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie. Les utilisateurs sont responsables de l'utilisation qu'ils font des ressources mises à leur disposition par l'ENSAIT.

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

ARTICLE 1 – CHAMP D'APPLICATION

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'ensemble des utilisateurs.

ARTICLE 2 – CONDITION D'UTILISATION DES SYSTEMES D'INFORMATION

2.1 Utilisation professionnelle / privée

Les communications électroniques (messagerie, internet…) sont des outils de travail ouverts à des usages professionnels administratifs, pédagogiques et de recherche et peuvent aussi constituer le support d'une communication privée.

L'usage des ressources est réservé à l'activité professionnelle pour les personnels et à la réalisation de travaux liés à l'exercice des missions de l'ENSAIT pour les autres utilisateurs.

L'utilisation des ressources à titre privé ne peut constituer qu'une simple tolérance, tant qu'elle ne porte pas atteinte à l'exercice de la mission de service public de l'ENSAIT.

Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet nommé « PRIVE ». La sauvegarde régulière des données à caractère privé incombera à l'utilisateur. La responsabilité de l'ENSAIT ne pourra être engagée quant à la conservation de cet espace. Toute information est réputée appartenir à l'ENSAIT à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée.

2.2 Continuité de service : gestion des absences et des départs

Afin d'assurer la continuité de service, l'utilisateur doit privilégier le dépôt de ses fichiers de travail sur des zones partagées par les membres de son service ou de son équipe.

Pour les personnels, le responsable devra prévoir le transfert des données professionnelles de l'utilisateur partant, en concertation avec celui-ci.

Les étudiants conservent des accès pendant six mois après la fin de leur inscription dans l'établissement. Ceux-ci seront fermés au-delà de cette date et les données supprimées. Les doctorants relèvent des règles relatives aux personnels dans la présente charte.

En tout état de cause les données non situées dans le répertoire « PRIVE » sont considérées comme des données appartenant à l'ENSAIT qui pourra en disposer.

ARTICLE 3 – PRINCIPES DE SECURITE

3.1 Règles de sécurité applicables

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

L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillant ou abusive. Cette mesure ne confère pas aux outils informatique protégés un caractère personnel. Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée.

La sécurité des systèmes d'information mis à sa disposition lui impose :

- De garde strictement confidentiels son (ou ses) code(s) d'accès et ne pas les dévoiler à un tiers.
- De respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.

Par ailleurs, la sécurité des ressources mises à disposition de l'utilisateur nécessite plusieurs précautions :

De la part de l'ENSAIT :

- Veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de continuité du service mises en place par la direction de l'ENSAIT.
- Limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.

De la part de l'utilisateur :

- S'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information pour lesquelles il n'a pas reçu d'habilitation explicite.
- Ne pas connecter directement au réseau local filaire des matériels autres que ceux confiés ou autorisés par l'ENSAIT.
- Ne pas installer, télécharger ou utiliser sur le matériel de l'ENSAIT, des logiciels ou progiciels sans respecter les droits de licence ; les logiciels doivent être utilisés dans les conditions des licences souscrites.
- Se conformer aux dispositifs mis en place par l'ENSAIT pour lutter contre les virus et les attaques par programmes informatiques.
- Ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies, vidéos ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

3.2 Devoirs de signalement et d'information

L'utilisateur doit avertir sa hiérarchie, dans les meilleurs délais, de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, suspicion d'une usurpation d'un code d'accès…etc.

Le responsable hiérarchique informera le Responsable de la Sécurité des Systèmes d'Information (RSSI rssi@ensait.fr) ainsi que le délégué à la protection des données de l'ENSAIT. (dpd@ensait.fr)

3.3 Mesures de contrôle de la sécurité

L'ENSAIT est dans l'obligation de mettre en place un système de journalisation[1] des accès au système d'information notamment Internet, messagerie et données échangées (mesures de volumétrie).

L'utilisateur est informé :

- Que pour effectuer la maintenance corrective, curative ou évolutive, l'ENSAIT se réserve la possibilité de réaliser des interventions (le plus souvent à distance) sur les ressources matérielles et logicielles mises à sa disposition.

[1] Conformément aux dispositions du décret n°2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne : conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur…etc.

- Qu'une maintenance à distance est précédée d'une information de l'utilisateur.
- Que toute situation bloquante pour le système ou générant une difficulté technique, pourra conduire à l'isolement du poste voire à la suppression des éléments en cause et éventuellement, la suspension du compte informatique.
- Que l'ensemble du système d'information peut donner lieu à une protection et un contrôle à des fins statistiques, de traçabilité réglementaire, de suivi fonctionnel, d'optimisation de sécurité ou de détection des abus, dans le respect de la législation applicable. Les données traitées dans ce cadre sont recueillies et gérées par des personnels habilités de la direction du numériques. Elles sont conservées pour une durée d'un an.
  Les droits correspondants à ces données (droit d'accès, de rectification, de suppression, de limitation et de portabilité) sont exercés auprès du délégué à la protection des données à l'adresse suivante : dpd@ensait.fr

Les personnels chargés du fonctionnement des systèmes d'informations sont soumis au secret professionnel (cf. *Charte informatique administrateurs*). Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que :

- Ces informations sont couvertes par le secret des correspondances[2] ou identifiées comme telles, elles relèvent de la vie privée de l'utilisateur.
- Elles ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité.
- Elles en tombent pas dans le champ de l'article 40 alinéa 2 du code de procédure pénale[3].

3.4 Avis de la Direction des Systèmes d'Information (DSI) avant l'acquisition de matériel informatique

Lorsqu'un personnel de l'ENSAIT souhaite acheter, dans le cadre de ses missions, du matériel informatique, ou logiciel, susceptible de se connecter au système d'information (ordinateur, périphérique informatique, matériel connecté au réseau de l'ENSAIT…) il sollicite la Direction des Système d'Information (DSI) afin d'obtenir un avis sur la qualité du matériel et/ou du logiciel et sa compatibilité au système d'information de l'ENSAIT.

En cas d'achat du matériel et/ou logiciel malgré un avis défavorable, le personnel utilisateur sera considéré comme responsable exclusif du matériel informatique et/ou logiciel concerné, et devra s'engager par écrit à en assumer l'entière responsabilité. la DSI ne pourra en aucun cas être considéré comme garant de l'utilisation qui en sera faite ni des conséquences de celle-ci.

Si la DSI considérait que la connexion de ce matériel et/ou logiciel au système d'information de l'ENSAIT pouvait faire courir des risques d'atteinte à la sécurité de celui-ci, l'accès de ce matériel et/ou logiciel au système d'information pourra, après information de la direction de l'ENSAIT, être limitée ou interdit.

[2] L'article 226-15 du Code pénal puni de 1an d'emprisonnement et de 45 000 € d'amende l'atteinte au secret des correspondances.
[3] Obligation faite à tout fonctionnaire d'informer sans délai le Procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions.

ARTICLE 4 – COMMUNICATIONS ELECTRONIQUES

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'ENSAIT.

4.2 Adresses électroniques

L'ENSAIT s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle ou scolaire 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.

Des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'utilisateurs, pourront être mis en place par l'ENSAIT.

4.3 Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations pourront être mises en place. En particulier des solutions de traitement des messages indésirables (spam, contrôle des virus…) seront déployées.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la législation sur la liberté d'expression ou portant atteinte à la dignité humaine ou à la vie privée.

4.4 Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1174 à 1177 du Code civil.

L'utilisateur doit en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels. Il doit en assurer la conservation dans le cadre de son activité professionnelle.

4.5 Internet

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (et par extension intranet) constitue l'un des éléments essentiel d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'institution.

Tout site web doit préciser les mentions légales et en particulier le respect des dispositions en matière de protection des données personnelles. Aucune publication de pages d'information à caractère privé sur les ressources du système d'information de l'ENSAIT n'est autorisée, sauf disposition particulière accordée et précisée par la direction.

L'ENSAIT se réserve le droit de filtrer ou d'interdire l'accès à certains sites web.

4.6 RENATER

Le réseau informatique de l'ENSAIT est également relié par l'intermédiaire du Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche (RENATER), ainsi l'ensemble des utilisateurs sont soumis à la Charte déontologique RENATER disponible à l'adresse suivante : https://www.renater.fr/telechargement%2C1392

Afin de bénéficier de ce réseau, l'ENSAIT s'est engagée à faire respecter les règles d'usage et de sécurité de la charte déontologique RENATER. Les trois points suivants sont essentiels et extraits de cette charte, ils imposent à l'ENSAIT de veiller à :

- L'utilisation à des fins strictement professionnelles du réseau, conformément à la finalité RENATER, à savoir l'enseignement, la recherche, les développements techniques, la diffusion de l'information scientifique et technique.
- L'utilisation rationnelle des ressources informatiques du réseau RENATER, de manière à éviter toute consommation abusive de ces ressources.
- L'utilisation loyale des ressources du réseau en prévenant et s'abstenant de toute utilisation malveillante ou malicieuse destinée à perturber ou porter atteinte au réseau RENATER.

4.7 Echange de fichiers

Tout téléchargement ou copie de fichiers (notamment sons, images, logiciels, cours en ligne…etc.), sur Internet ou localement doit s'effectuer dans le respect des droits de la propriété intellectuelle et de la réglementation relative à la protection des données à caractère personnel (transfert d'un fichier comportant des données personnelles : nom, prénom, date de naissance, photo ou vidéo…etc).

L'ENSAIT se réserve le droit de limiter le téléchargement ou la copie de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'ENSAIT, codes malveillants, programmes espions, phishing…).

L'ENSAIT rappelle que l'utilisation des ressources implique un respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement des tous les tiers titulaires de tels droits.

ARTICLE 5 – RESPECT DES DISPOSITION LEGALES SUR LA PROTECTION DES DONNES PERSONNELLES

L'utilisateur est informé de l'obligation de respecter les dispositions légales en matière de traitement automatisé des données à caractère personnel, conformément au Règlement Général sur la Protection des Données (RGPD-2016/679), et à la loi n°2008-493 du 20 juin 2018 relative à la protection des données personnelles.

Les données à caractère personnel sont des informations qui permettent, sous quelque forme que ce soit, d'identifier directement ou indirectement les personnes physiques à qui elles appartiennent.

Les traitements de données à caractère personnel consistent en toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction…).

Tous les traitements de données à caractère personnel sont soumis aux obligations et formalités préalables prévues par la législation sur la protection des données.

Voir « *Politiques RGPD ENSAIT (personnels, usagers, partenaires »*.

ARTICLE 6 – LIMITATION DES USAGES

Tout abus dans l'utilisation des ressources mises à disposition de l'utilisateur à des fins extra-professionnelles, est passible de sanction disciplinaires et pénales.

En cas de non-respect des règles définies dans la présente charte, le Directeur de l'ENSAIT pourra, sans préjuger des poursuites ou procédures de sanction pouvant être engagées à l'encontre des personnels, suspendre les autorisations d'accès aux ressources informatiques.