université de TOURS | Direction des systèmes d'information

Charte d'usage des Systèmes d'Information

Préambule

Les "systèmes d'information" recouvrent l'ensemble des moyens mis en œuvre par l'Université de Tours pour opérer les services nécessaires à ses missions et qui traitent les informations de Gestion, d'Enseignement et de Recherche.

L'informatique nomade, tels que les assistants personnels, les ordinateurs portables, les téléphones portables..., est également un des éléments constitutifs des systèmes d'information.

Le terme « d'utilisateur » recouvre toute personne ayant vocation à détenir un compte informatique ou à avoir accès aux ressources des systèmes d'information quel que soit son statut.

Il s'agit notamment de :

- *Tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'enseignement et de la recherche ;*
- *Tout étudiant inscrit dans l'établissement ;*
- *Toute personne extérieure à l'établissement, visiteur, invité, prestataire[1] ayant contracté avec l'établissement.*

Le bon fonctionnement des systèmes d'information suppose le respect des dispositions législatives et réglementaires, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

La présente charte définit les règles d'usage et de sécurité que l'établissement et l'utilisateur s'engagent à respecter : elle précise les droits et les devoirs de chacun.

Engagements de l'établissement

L'établissement porte à la connaissance de l'utilisateur la présente charte.

L'établissement met en œuvre toutes les mesures nécessaires pour assurer la sécurité des systèmes d'information et la protection des utilisateurs.

L'établissement s'engage à respecter la Charte déontologique RENATER.

L'établissement facilite l'accès des utilisateurs aux ressources des systèmes d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'établissement est tenu de respecter l'utilisation résiduelle des systèmes d'information à titre privé.

Engagements de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait des systèmes 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[2].

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

L'utilisation des ressources qui sont mises à sa disposition doit être rationnelle et loyale afin d'en éviter la saturation ou le détournement à des fins personnelles.

Article I. Champ d'application

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

Ces règles s'appliquent à toute personne autorisée à utiliser les moyens informatiques de l'établissement, y compris les moyens informatiques mutualisés ou externalisés, et s'étendent aux réseaux extérieurs accessibles par l'intermédiaire des réseaux de l'établissement.

Article II. Droit d'accès aux systèmes d'information

Le droit d'accès aux systèmes d'information est temporaire. Il est retiré si la qualité de l'utilisateur ne le justifie plus et, sauf retraités et personnels sortants[3], au plus tard 6 mois après que celui-ci n'ait plus vocation à détenir un compte informatique.

Il peut également être retiré, par mesure conservatoire, si le comportement de l'utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.

Article III. Conditions d'utilisation des systèmes d'information

Section III.1 Utilisation professionnelle / privée

L'utilisation des systèmes d'information de l'établissement a pour objet exclusif de mener des activités de recherche, d'enseignement, de documentation, d'administration ou de vie universitaire. Sauf autorisation, ces moyens ne peuvent être employés en vue d'une utilisation ou de la réalisation de projets ne relevant pas des missions de l'établissement ou des missions confiées aux utilisateurs. Ils peuvent néanmoins constituer le support d'une communication privée dans les conditions décrites ci-dessous.

L'utilisation résiduelle des systèmes d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée.

Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement[4] à cet effet ou en mentionnant le caractère personnel sur la ressource[5]. La protection et la sauvegarde régulière des données à caractère privé incombent à l'utilisateur.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif de l'établissement, il lui appartient 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. La sauvegarde des données stockées sur le poste de travail de l'utilisateur relève de la responsabilité de chaque utilisateur. Il est rappelé que celle-ci

1 Le contrat devra prévoir expressément l'obligation de respect de la charte.
2 Notamment le secret médical dans le domaine de la santé.
3 Relevé de décision concernant la « Définition des services numériques pour les retraités » du 11 avril 2012
4 Le dossier devra être impérativement nommé «PERSONNEL».
5 Pour exemple, "_personnel_nom_de_l_objet_" : l'objet pouvant être un message, un fichier ou toute autre ressource numérique. Arrêt n°2044 du 21 octobre 2009 (07-43.877) de la Cour de cassation, chambre sociale.

ne concerne pas les données sensibles qui doivent être traitées sur le serveur bureautique.

L'utilisation des systèmes d'information à titre privé doit respecter la réglementation en vigueur. En particulier, la détention, diffusion et exportation d'images à caractère pédophile[6], ou la diffusion de contenus à caractère raciste ou antisémite[7] est totalement interdite.

Par ailleurs, eu égard à la mission de l'établissement, la consultation de sites de contenus à caractère pornographique depuis les locaux de l'établissement, hors contexte professionnel, est interdite.

L'utilisateur se doit de respecter les principes de neutralité religieuse, politique et commerciale.

Section III.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.

En cas de départ, ou d'absence prolongée, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition. En tout état de cause les données non situées dans un espace identifié comme personnel, sont considérées comme appartenant à l'établissement qui pourra en disposer.

Article IV. Principes de sécurité

Section IV.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 codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive.

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 respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ; chaque utilisateur est responsable de l'utilisation qui en est faite ;*
- *De garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers. Il en est de même pour le(s) badge(s) ;*
- *De respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès ou un badge d'un autre utilisateur, ni chercher à les connaître ;*
- *De veiller à ne pas laisser leur poste de travail en libre accès.*

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 :

- *S'interdire d'accéder ou de tenter d'accéder à des ressources des systèmes d'information, pour lesquelles il n'a pas reçu d'habilitation explicite ;*
- *Ne pas connecter directement aux réseaux filaires des matériels autres que ceux confiés ou autorisés par l'établissement ;*
- *Ne pas installer, télécharger ou utiliser sur le matériel de l'établissement, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de l'établissement ;*
- *Se conformer aux dispositifs mis en place par l'établissement pour lutter contre les virus et les attaques par programmes informatiques ;*
- *S'engager à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou du logiciel ;*
- *Veiller à protéger les matériels mis à sa disposition contre le vol et les dégradations ;*
- *Appliquer les recommandations sécurité de l'établissement.*

Section IV.2 Devoirs de signalement et d'information

L'utilisateur doit avertir le responsable de la sécurité des systèmes d'information dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans les systèmes d'information, etc. Il signale également à son responsable ou sa hiérarchie toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

Section IV.3 Mesures de contrôle

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 maintenance à distance est précédée d'une information de l'utilisateur ;*
- *Que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée ; le cas échéant supprimée.*
- *Que les systèmes d'information donnent lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.*

Les personnels chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel. 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 ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur ;*
- *Elles ne mettent pas en cause le bon fonctionnement technique des applications ou leur sécurité ;*
- *Elles ne tombent pas dans le champ de l'article[8] 40 alinéa 2 du code de procédure pénale.*

Article V. Communication électronique

Section V.1 Messagerie électronique

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

6 Article L 323-1 et s. du Code pénal
7 Article 24 et 26bis de la Loi du 29 juillet 1881
8 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.

(a) Adresses électroniques

L'établissement s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative est ensuite de la responsabilité de l'utilisateur.

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.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur 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 listes ne peuvent être utilisées sans autorisation.

(b) Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé[9] ou s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place. En particulier des solutions de traitement des messages indésirables (spam, contrôle des virus...) pourront être 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 loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques...).

Les échanges électroniques (courriers, forums de discussion, etc.) se doivent de respecter la correction normalement attendue dans tout type d'échange tant écrit qu'oral.

La transmission de données classifiées [10] est interdite sauf dispositif spécifique agrée et la transmission de données dites sensibles doit être évitée ou effectuée sous forme chiffrée.

(c) Émission et réception des messages

L'utilisateur doit faire preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes, ...).

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.

(d) 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[11] 1369-1 à 1369-11 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.

(e) 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.

Section V.2 Internet

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

Internet est un outil de travail ouvert à des usages professionnels (administratifs, pédagogiques ou de recherche). Si une utilisation résiduelle privée, telle que définie en section III.1, peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'établissement sont présumées avoir un caractère professionnel.

(a) Publication sur les sites internet et intranet de l'établissement

Toute publication d'information sur les sites internet ou intranet de l'établissement[12] doit être validée par le responsable de publication nommément désigné.

Aucune publication d'information à caractère privé (pages privées ...) sur les ressources des systèmes d'information de l'établissement n'est autorisée, sauf disposition particulière précisée dans un guide d'utilisation établi par le service ou l'établissement.

(b) 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.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'établissement. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou l'établissement.

Section V.3 Téléchargements

Tout téléchargement ou copie de fichiers (notamment sons, images, logiciels, cours en ligne...) sur Internet ou localement doit s'effectuer dans le respect des droits de propriété intellectuelle tels que définis à l'article VII.

L'établissement 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, codes malveillants, programmes espions ...).

Article VI. Traçabilité

L'établissement est dans l'obligation légale de mettre en place un système de journalisation[13] des accès Internet, de la messagerie et des données

9 Pour exemple, les messages comportant les termes ("privé") dans l'objet ou sujet du message
10 Il s'agit des données classifiées de défense qui couvre le «confidentiel défense », le «secret défense» et le «très secret défense »
11 Issus de la loi n° 2004-575 du 21 juin 2004, ces articles fixent certaines obligations pour la conclusion des contrats en ligne
12 A partir des ressources informatiques mises à la disposition de l'utilisateur.
13 Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur…

échangées.

L'établissement se réserve le droit de mettre en place des outils de traçabilité sur tous les systèmes d'information.

Article VII. Respect de la propriété intellectuelle

L'établissement rappelle que l'utilisation des ressources informatiques[14] 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 ;*
- *ne pas 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 ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.*

Article VIII. Respect de la loi informatique et libertés

L'utilisateur à l'obligation de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée et au Règlement général européen sur la protection des données (RGPD).

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.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi « Informatique et Libertés » et le RGPD.

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement à sa mise en œuvre le Correspondant Informatique et Libertés (CIL) désigné par l'Établissement à la Commission Nationale Informatique et Libertés. Il remplit le fichier créé à cet effet, celui-ci étant disponible sur demande auprès du CIL (daj@univ-tours.fr).

La création d'un fichier de traitement de données doit respecter les principes édictés par la Loi Informatique et Libertés ainsi que le RGPD. Notamment, il est interdit, sauf exception strictement encadrée par l'article 8 de la loi Informatique et Libertés, de recueillir des données relatives à la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale d'une personne physique, de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou la vie sexuelle ou encore l'orientation sexuelle d'une personne physique.

Conformément au RGPD, les personnes concernées par un traitement informatique portant sur leurs données à caractère personnel seront dûment informées :

- que le responsable du traitement au sein de l'établissement est le président de l'université ;

- la finalité de la collecte de données ;

- la base juridique du traitement ;

- le but précis du traitement ;

- le type de données recueillies ainsi que les moyens mis en œuvre pour les recueillir ;

- les destinataires des catégories de données ;

- la durée de conservation des données ou à défaut les critères utilisés pour déterminer cette durée ;

- le droit d'accès aux données fondé sur les articles 38, 39, 40 et 40-1 de la loi n°78-17 du 6 janvier 1978 ainsi que la personne à contacter pour accéder à ces données ;

- le droit de déposer une réclamation auprès de la CNIL en cas de besoin ;

- le droit d'opposition, de rectification voire de retrait du consentement lorsque cela est possible.

Ces informations doivent être clairement communiquées à toutes personnes concernées, en amont du début du traitement. Elles doivent l'être également, à tout moment, en cas de demande à l'autorité compétente par ces mêmes personnes.

Article IX. Limitation des usages

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation établis par le service ou l'établissement, la «personne juridiquement responsable» de l'établissement pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des utilisateurs, limiter les usages par mesure conservatoire.

Par «personne juridiquement responsable», il faut entendre toute personne ayant la capacité de représenter l'établissement (président d'université, directeur d'institut...).

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extra-professionnelles est passible de sanctions.

Article X. Entrée en vigueur de la charte

Le présent document annule et remplace tous les autres documents ou chartes relatifs à l'utilisation des systèmes d'information de l'établissement. Il est susceptible de modification.

Il est annexé au règlement intérieur.

Mention à porter à la main : « Je soussigné(e) (Nom, Prénom) atteste avoir lu le présent règlement et m'engage à le respecter. »

Je soussigné(e) : _____

_____

Fait à :

Le Signature :

14 Y compris les ressources pédagogiques.