Charte d'usage du système d'information

université angers

Sommaire

Préambule

Le système d'information de l'établissement est un outil de travail réservé aux usages professionnels pouvant, à titre résiduel et suivant les dispositions prévues à cette charte, être le support d'une utilisation relevant de la vie privée de l'utilisateur.

La pluralité des lieux de travail (et notamment l'accès de l'extérieur de l'établissement aux ressources du système d'information) n'altère en rien le caractère professionnel du système d'information.

Le bon fonctionnement du système 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'usages et de sécurité que l'établissement et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun.

Elle n'a pas pour objet et objectif de couvrir de façon exhaustive tous les cas de figure pouvant se présenter dans le cadre de l'utilisation des moyens informatiques et de communication électronique mis à la disposition par l'établissement. C'est dans l'esprit des règles présentées dans ce document que chacun devra se conformer dans des situations non envisagées.

La présente charte est susceptible d'évoluer en fonction du contexte réglementaire, légal ou technologique.

Les règles d'usage et de sécurité s'appliquent à l'établissement ainsi qu'à l'ensemble des utilisateurs. Un guide juridique annexé à la présente Charte rappelle les dispositions législatives en vigueur pour son application. Elle est complétée par le guide technique utilisateur à disposition de chaque utilisateur définissant les principales règles pratiques d'usage.

II. Champs d'application

Par "système d'information" s'entend l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'université d'Angers.
Les outils de la mobilité (tels que les ordinateurs portables, les téléphones portables…) mis à disposition par l'établissement sont également des éléments constitutifs du système d'information.

Par «établissement», s'entend l'**université d'Angers**.

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

Ainsi sont notamment désignés :

- tout agent titulaire, non titulaire ou bénéficiant d'une convention de stage, concourant à l'exécution des missions du service public de l'enseignement supérieur et de la recherche ;
- tout prestataire[1] ayant contracté avec l'établissement ;
- tout étudiant inscrit dans l'établissement ;
- toute personne autorisée à accéder à un service numérique.

III. Portée et opposabilité

La présente charte est annexée au règlement intérieur de l'établissement.
L'établissement est tenu de la porter à la connaissance de l'utilisateur et en conséquence, l'utilisateur est supposé en avoir pris connaissance.

➔ RESPONSABILITES ET ENGAGEMENTS DE L'ETABLISSEMENT

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

L'établissement met en œuvre les mesures pour assurer la sécurité du système d'information et la protection des utilisateurs.

L'établissement facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont à usage professionnel mais l'établissement est tenu de respecter la vie privée de chacun.

Un responsable de la sécurité des systèmes d'information (RSSI) et un correspondant informatique et libertés (CIL) sont désignés au sein de l'établissement. L'utilisateur pourra s'adresser à ces agents pour tout complément d'information.

➔ RESPONSABILITES ET ENGAGEMENTS DE L'UTILISATEUR

L'utilisateur est responsable, en toutes circonstances, de l'usage qu'il fait du système d'information auquel il a accès.

L'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat. 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. Le non-respect de ses obligations ou tout abus dans l'utilisation des ressources mises à sa disposition engagent la responsabilité de l'utilisateur et peut donner lieu à des procédures disciplinaires ou des poursuites pénales. Sans préjuger des poursuites ou procédures engagées, l'établissement peut limiter, par mesure conservatoire, l'usage du système d'information pour l'utilisateur concerné.

III. Principes de sécurité

1. REGLES DE SECURITE APPLICABLES

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

Les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques 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 du système 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 précisées dans le guide technique utilisateur ;
- de garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers (sauf cas prévus en section V.2) ;
- 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 la disposition de l'utilisateur nécessite plusieurs obligations :

- 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 (Cf. section V.2) ;
- 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 aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'établissement, ou ceux dont la liste a été précisée dans un guide d'utilisation établi par le service ou l'établissement ;
- ne pas installer, télécharger ou utiliser sur les matériels 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 sa hiérarchie ;
- se conformer aux dispositifs mis en place par l'établissement pour lutter contre les virus et les attaques par programmes informatiques mentionnés dans le guide technique utilisateur ;

2. DEVOIRS D'INFORMATION

L'établissement doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre de sécuriser son utilisation du système d'information. L'utilisateur peut s'adresser au responsable de la sécurité des systèmes d'information (RSSI) et au correspondant informatique et libertés (CIL) notamment pour compléter son information ou répondre à ses questions.

L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte (un défaut de sécurité, une intrusion dans le système d'information, …). Il signale également à la personne responsable de la gestion du système d'information (et à défaut au RSSI) toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

3. MESURES DE CONTROLE DE LA SECURITE

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 la disposition de l'utilisateur ;

toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée ; le cas échéant, elle sera supprimée.

Le système d'information peut donner 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 du système d'information sont soumis à des règles de confidentialité renforcées, notamment dans le cadre d'un engagement d'éthique et de déontologie. 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 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 ne tombent pas dans le champ de l'article[2] 40 alinéa 2 du code de procédure pénale.

V. Conditions d'utilisation du système d'information

1. UTILISATION PROFESSIONNELLE / PRIVEE

Toute donnée gérée au sein du système d'information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée.

Les ressources (ordinateur, téléphone, …) et les outils de communications électroniques (messagerie, internet …) sont des outils de travail réservés à un usage professionnel et peuvent également constituer, à titre résiduel, le support d'une utilisation ou communication privée.

- L'utilisation résiduelle à titre privé des ressources et outils mis à disposition de l'utilisateur doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. L'utilisation à titre privé (en temps et en coût généré) doit demeurer négligeable par rapport aux usages professionnels.
- 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.

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 ou en mentionnant le caractère privé sur la ressource.
Le nom de cet espace ou de la ressource (messages, fichiers,…) doit s'intituler « **privé** » pour que soit appliqué le principe du secret des correspondances (voir le guide juridique en annexe).

2. CONTINUITE DE SERVICE, GESTION DES ABSENCES ET DES DEPARTS

Pour un besoin de continuité du service avéré par une nécessité d'intérêt général détaillée par écrit et sur demande explicite de sa hiérarchie, l'utilisateur doit fournir les modalités[3] permettant l'accès aux ressources mises spécifiquement à sa disposition.

Lors de son départ définitif de l'établissement :

- L'utilisateur ne peut détruire tout ou partie de ses données professionnelles sans avis de sa hiérarchie. Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de l'établissement ;
- il appartient à l'utilisateur de détruire son espace ou ses données à caractère privé, la responsabilité de l'établissement ne peut être engagée quant à la conservation de ces données après son départ.

3. STOCKAGE ET ARCHIVAGE

S'agissant d'archives publiques, les documents produits par les agents dans l'exercice de leur fonction sont des archives publiques. Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des documents pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve constitutifs de son activité professionnelle.

IV. Communications électroniques

1. MESSAGERIE ELECTRONIQUE ET OUTILS DE TRAVAIL COLLABORATIF

L'utilisation de la messagerie constitue l'un des éléments d'optimisation du travail, de mutualisation et d'échange de l'information au sein de l'établissement. Les règles définies ci-dessous s'appliquent également aux outils de travail collaboratif généralement liés à la messagerie de l'établissement.

2. ADRESSES ELECTRONIQUES

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'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[4] nominative est attribuée à un utilisateur qui la gère sous sa responsabilité.

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 relève de la responsabilité exclusive de l'établissement.

3. CONTENU DES MESSAGES ELECTRONIQUES

Tout message est réputé professionnel sauf s'il comporte dans son objet une mention particulière et explicite indiquant son caractère privé[5] ou bien s'il est stocké dans un espace privé de messages ou de données.

4. ÉMISSION ET RECEPTION DES MESSAGES

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 de limiter les diffusions inutiles de messages en masse.

5. STATUT ET VALEUR JURIDIQUE DES MESSAGES

Tout message électronique échangé avec des tiers peut engager la responsabilité, au plan juridique, de l'établissement. L'utilisateur doit, en conséquence, être particulièrement attentif sur la nature des messages électroniques qu'il échange et à ne s'engager par messagerie que s'il est habilité à le faire.

6. INTERNET

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

L'établissement met, dans la mesure du possible, un accès Internet à la disposition de l'utilisateur.

Internet est un outil de travail réservé à un usage professionnel et, à titre résiduel, à un usage privé (tel que défini à l'article V.1) dans le respect de la législation en vigueur.

En complément des dispositions légales en vigueur et au regard de la mission de l'établissement, la consultation de sites à caractère pornographique depuis les locaux de l'établissement ou par utilisation des ressources de l'établissement est interdite.

7. PUBLICATIONS SUR LES SITES INTERNET ET INTRANET DE L'ETABLISSEMENT

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.

Aucune publication de pages d'information à caractère privé (pages privées…) sur les ressources du système d'information de l'établissement n'est autorisée, sauf disposition particulière précisée par l'établissement, par exemple dans les conditions d'utilisation de la plateforme de blogs de l'Université.

8. SECURITE

L'établissement se réserve le droit de filtrer ou d'interdire l'accès à certaines ressources numériques, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes. L'utilisateur en est informé.

9. RESEAUX SOCIAUX

Les réseaux sociaux externes à l'établissement (exemple : Facebook, Linkedin, Viadeo…) occupent une place de plus en plus importante dans la sphère professionnelle.
Ils permettent à l'établissement et à chaque agent de créer et de gérer des relations professionnelles et d'optimiser la communication et les actions « marketing ».
Dès lors que son appartenance à l'établissement transparaît dans son utilisation d'un réseau social, l'utilisateur est informé que toute information publiée relative à l'établissement, son activité, etc… relève d'une communication au sein de la sphère professionnelle.

Ainsi, dès lors que le réseau social est le support d'un usage à caractère professionnel, l'utilisateur doit :

- Utiliser un profil mettant explicitement en évidence son identité (Nom, prénom, fonction, …) ;
- Appliquer les mêmes règles d'usage et de déontologie que celles décrites dans les sections ci-dessus (notamment III, V.1 et V.2) et veiller au respect de son obligation de réserve ;
- S'abstenir de créer un profil générique relatif à l'établissement ou une de ses activités sans autorisation explicite du président ou du directeur général des services de l'établissement.

10. TELECHARGEMENTS

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect de la réglementation en vigueur.

L'établissement se réserve le droit de limiter le téléchargement 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'établissement, codes malveillants, programmes espions, …).

V. Traçabilité

L'établissement se réserve le droit de mettre en place des outils de traçabilité d'utilisation du système d'information.
En application de la loi n° 2004-575 du 21 juin 2004, l'établissement doit mettre en place un système de journalisation[8] des accès Internet, de la messagerie et des données échangées. Ces outils de traçabilité sont mises en œuvre suivant les recommandations de la Commission nationale de l'informatique et des libertés (CNIL), notamment la durée de conservation des traces.

VI. Respect de la propriété intellectuelle

Les systèmes d'information ne doivent en aucune manière être utilisés à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin, tels que des textes, images, photographies, œuvres musicales, œuvres audiovisuelles, logiciels et jeux vidéo, sans l'autorisation des titulaires des droits prévue aux livres Ier et II du code de la propriété intellectuelle lorsque cette autorisation est requise.

L'établissement, titulaire d'un accès à Internet, est tenu, en application de l'article L. 336-3 du code de la propriété intellectuelle, de mettre en œuvre les moyens nécessaires pour que l'accès Internet ne soit pas utilisé à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin. La loi prévoit qu'en cas de non-respect de cette obligation, le titulaire de l'accès Internet peut voir sa responsabilité pénale engagée au titre de la négligence caractérisée[2].

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 écrite des titulaires de ces droits.

L'établissement pourra mettre en œuvre les mesures de contrôle appropriées au respect de cette clause.

VII. Respect de la loi « informatique et libertés »

L'établissement veille à une stricte application de la loi « informatique et libertés ».

L'utilisateur doit 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 modifiée, dite «Informatique et Libertés» consultable sur le site de la CNIL (www.cnil.fr). Le guide juridique annexé à la présente charte précise les termes de la loi. L'utilisateur peut se référer au CIL de l'établissement pour tout complément d'information.

VIII. Entrée en vigueur de la charte

La présente charte a été approuvée au CA de l'université d'Angers du 29/01/2015.

1 Le contrat devra prévoir expressément l'obligation de respect de la charte ;

2 Précisé dans le guide juridique en annexe (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 …)

3 A titre d'exemple, il doit communiquer sur demande de sa hiérarchie le moyen d'accéder à son ordinateur professionnel.

4 L''adresse est de la forme prénom.nom @ <univ-angers.fr ou etud.univ-angers.fr>

5 Pour exemple, les messages comportant (« privé ») dans l'objet du message.

6 Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur …

7 Cette contravention est punie d'une peine d'amende d'un montant maximum de 1500 euros pour les personnes physiques et 7500 euros pour les personnes morales, qui peut être assortie d'une peine de suspension de l'accès à internet d'une durée maximum d'un mois. Ces sanctions sont prononcées par le juge judiciaire.