Règlement Intérieur

Approuvé par le CA du 05 juin 2014

Mis à jour le 22 mai 2025

(EXTRAIT)

Charte d'usage du système d’information

10BSommaire

I - 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·rice.

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·rice s'engagent à respecter : elle précise les droits et devoirs de chacun.e.

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.e 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·trices. Un guide juridique rappelle les dispositions législatives en vigueur pour son application. Elle est complétée par le « guide technique de l'utilisateur du système d'information » à disposition de chaque utilisateur·rice définissant les principales règles pratiques d'usage.

Elle est également complétée par le document « Politique de Sécurité des Systèmes d'information » (PSSI) au sein de l'Université d'Angers.

Ces documents sont consultables sur le site de l'Université d'Angers dans la page web publique décrivant le système d'information de l'Université d'Angers.

II - Champs d'application

Par "système d'information" s'entend l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux informatiques ou 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·rice», 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.es :

- 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.e inscrit.e dans l'établissement ;

- Toute personne autorisée à accéder à un service numérique de l'établissement.

III - Portée et opposabilité

La présente charte est intégrée au titre 8 du règlement intérieur de l'établissement.

L'établissement est tenu de la porter à la connaissance de l'utilisateur·rice et en conséquence, l'utilisateur·rice est supposé·e en avoir pris connaissance.

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

Responsabilités et engagements de l'établissement

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

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

L'établissement facilite l'accès des utilisateurs·rices 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.e.

Un/Une responsable de la sécurité des systèmes d'information (RSSI) et un/une Délégué.e à la protection des données (DPD) sont désignés au sein de l'établissement. L'utilisateur·rice pourra s'adresser à cet (ou ces) agent (s) pour tout complément d'information.

Responsabilités et engagements de l'utilisateur·rice

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

L'utilisateur·rice est soumis.e au respect des obligations résultant de son statut ou de son contrat. Il/Elle a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il/elle 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·rice 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·rice concerné·e.

IV - Principes de sécurité

1. Règles de sécurité applicables

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

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·rice 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 de l'utilisateur du système d'information » ;
- 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) ;
- Respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un/une autre utilisateur·rice, ni chercher à les connaître.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur·rice 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·rice est expressément habilité·e ;

✓ De la part de l'utilisateur·rice :

- 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 aux réseaux filaires locaux des matériels autres que ceux autorisés explicitement par 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 de l'utilisateur du système d'information ».

2. Devoirs d'information

L'établissement doit porter à la connaissance de l'utilisateur·rice tout élément susceptible de lui permettre de sécuriser son utilisation du système d'information. L'utilisateur peut s'adresser au/à la responsable de la sécurité des systèmes d'information (RSSI) et au/à la Délégué.e à la protection des données (DPD) notamment pour compléter son information ou répondre à ses questions.

L'utilisateur·rice 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/Elle 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 contrôle de la sécurité

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·rice.

Tout élément bloquant ou générant une difficulté technique sera isolé et le cas échéant supprimé.

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/Elles ne peuvent divulguer les informations qu'ils/elles sont amenés.es 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·rice ;
- 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 / privée

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

Les ressources (ordinateur, téléphone, …) de l'université d'Angers et les outils de communications électroniques (messagerie, navigateur internet …) associés 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·rice 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·rice, au temps qu'il/elle y consacre et au bon fonctionnement du service.

Il appartient à l'utilisateur·rice 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 pour que soit appliqué le principe du secret des correspondances (voir l'annexe juridique).

Le nom de cet espace ou de la ressource (messages, fichiers, etc) peut par exemple s'intituler **« privé »**

PROPOSITIONS AJOUTS ET DEPLACEMENTS FEVRIER 2023

2. Continuité de service, gestion des absences

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·rice doit fournir les modalités[3] permettant l'accès aux ressources mises spécifiquement à sa disposition (code d'accès, nom d'utilisateur·rice, etc…).

3. Stockage et archivage

Les documents ou données produits par les agents dans l'exercice de leur fonction sont des archives publiques. Chaque utilisateur.rice 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.

Lors de son départ définitif de l'établissement :

- L'utilisateur·rice ne peut détruire tout ou partie de ses données *non privées* sans avis *des personnes responsables de son activité*. Les mesures de conservation des données non privées sont définies *par* le/la responsable désigné.e au sein de l'établissement ;

[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 les mots de passe d'accès à son ordinateur professionnel.

- il appartient à l'utilisateur·rice 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.

4. Conservation des accès aux ressources numériques

Les accès aux ressources numériques sont définis en fonction du statut ou contrat de l'utilisateur·rice et de l'activité qu'il/elle exerce au sein de l'établissement.

Lorsqu'elle quitte l'établissement la personne perd sa qualité d'utilisateure·rice. Il/Elle doit prendre toute disposition afin de conserver ses données personnelles avant la clôture effective de ses accès aux ressources numériques.
Des procédures particulières sont mises en œuvre, en fonction du statut ou contrat de l'utilisateur·rice et de l'activité qu'il/elle exerce au sein de l'établissement, afin de l'informer avant son départ de la date effective à laquelle il/elle n'aura plus accès aux ressources numériques telles qu'il/elle avait pendant sa période d'activité.
La date de clôture effective peut être postérieure à la date de fin d'activité . Elle ne peut être prolongée plus de six mois après la date de fin d'activité et doit être la plus proche possible de celle-ci.

VI - Communications électroniques

1. Messagerie électronique et outils de travail collaboratif

L'utilisation de la messagerie électronique 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 électroniques

L'établissement s'engage à mettre à la disposition de l'utilisateur·rice une adresse 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[4] nominative est attribuée à un utilisateur·rice qui la gère sous sa responsabilité. Il/Elle l'utilise avec précaution et l'emploie essentiellement pour des échanges en lien avec son activité professionnelle.

Une adresse électronique « fonctionnelle » ou « organisationnelle », peut être mise en place pour un utilisateur·rice ou un groupe d'utilisateurs·rices 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 électroniques

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] 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.

4. Émission et réception des messages

L'utilisateur·rice doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

Il/Elle 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·rice doit, en conséquence, être particulièrement attentif/attentive sur la nature des messages électroniques qu'il/elle échange et à ne s'engager par messagerie que s'il/elle est habilité.e à le faire.

6. Usage d'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·rice.

Internet est un outil de travail réservé à un usage professionnel ou pédagogique et, à titre résiduel, à un usage privé 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.

Il est interdit de se livrer depuis des matériels appartenant à l'université d'Angers ou depuis le réseau informatique de l'établissement à des actes mettant sciemment en péril la sécurité ou le fonctionnement de systèmes d'informations locaux ou distants.

7. Publications sur les sites internet et intranet 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.e.

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. Sécurisation des accès aux ressources

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.

9. Réseaux 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·rice est informé·e 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·rice 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/de la président·e ou du/de la directeur·rice général·e des services de l'établissement.

10. Téléchargements

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 du système d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'établissement, codes malveillants, programmes espions, …).

VII - Traçabilité

L'établissement a mis en place des outils de traçabilité d'utilisation du système d'information en conformité avec les dernières lois qui régissent ces obligations.
La durée de conservation des journaux informatiques est de un an maximum. L'établissement s'interdit de les exploiter au-delà de trois mois sauf sur réquisition officielle ou sous une forme rendue anonyme.
Conformément au Règlement Général de Protection des Données promulgué par l'UE, une personne est désignée par l'UA comme Délégué à la Protection des Données (DPD) et contrôle le respect du RGPD notamment vis à vis de la conservation et mise à disposition des données.

VIII - Respect de la propriété intellectuelle

Le système d'information ne doit en aucune manière être 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, 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/la titulaire de l'accès Internet peut voir sa responsabilité pénale engagée au titre de la négligence caractérisée[6].

En conséquence, chaque utilisateur·rice 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.

IX - Préservation de l'intégrité du système d'information

L'utilisateur.rice s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux par l'usage anormal de matériels ou de logiciels.
Il/elle s'engage à ne pas tenter d'accéder aux informations qui ne lui sont pas destinées quand bien même celles-ci ne seraient pas suffisamment protégées.

Il/elle s'engage notamment à :

- ne pas développer, installer ou copier des programmes destinés à contourner la sécurité ou saturer les ressources ;
- ne pas introduire volontairement de programmes nuisibles (virus, cheval de Troie, ver...) ;
- L'utilisateur.rice contribue à son niveau à la sécurité du système d'information. A ce titre, il/elle fait preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes, hameçonnage, ...).

X - Matériel personnel

Les moyens informatiques personnels (ordinateurs, smartphones, tablettes, etc.) de possession privée, lorsqu'ils sont utilisés pour accéder au système d'information de l'université d'Angers, ne doivent pas remettre en cause ou affaiblir les politiques de sécurité en vigueur dans l'université par une protection insuffisante ou une utilisation inappropriée.

L'utilisateur·rice protège les équipements personnels qu'il/elle utilise pour accéder - à distance ou à partir du réseau wifi de l'UA - au système d'information de l'université d'Angers. Il est recommandé de ne pas stocker sur son matériel personnel des données en provenance du système d'information de l'UA et qui pourraient en cas de divulgation externe nuire au bon fonctionnement de celui-ci. En cas de perte ou vol d'un matériel personnel qui comportait des données professionnelles non publiques en lien avec le système d'information de l'UA, l'utilisateur·rice doit le signaler le plus rapidement possible au/à la responsable de la sécurité des systèmes d'information (RSSI) afin d'étudier ensemble les risques induits par cette perte.

[6] 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.

XI - Respect de la loi « informatique et libertés »

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

L'utilisateur·rice 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·rice peut se référer au CIL de l'établissement pour tout complément d'information.

XII - Entrée en vigueur de la charte

La présente charte a été approuvée au CA de l'université d'Angers du 22/05/2025