

Charte régissant l'usage professionnel du système d'information de l'université de Toulon

1. Objet et champ d'application

Un **système d'information** peut être défini comme l'ensemble organisé de ressources (personnes, données, procédures, matériels, logiciels, etc.) permettant de traiter et diffuser de l'information en fonction des objectifs d'une organisation.

Les **ressources informatiques** sont les réseaux, les serveurs, les stations de travail, les logiciels, les applications, les bases de données, etc., c'est une partie du système d'information. L'informatique nomade, tels que les assistants personnels, les ordinateurs portables, les téléphones portables..., est également un des éléments constitutifs du système d'information.

Le terme **utilisateur** désigne la personne agissant sur le système d'information, ici toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information de l'université de Toulon quel que soit son statut. Il s'agit notamment de :

- tout agent titulaire ou non titulaire concourant à l'exécution des missions de l'université ;
- tout prestataire sous contrat avec l'université ;
- tout stagiaire ayant contracté une convention de stage avec l'un des services ou l'une des composantes de l'UTLN ;
- toute personnalité invitée dans le cadre des missions du service public de l'enseignement supérieur et de la recherche par l'une des composantes ou l'un des services de l'université.

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 a pour objet de définir les règles d'usage et de sécurité que l'université de Toulon et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun.

Ces règles s'étendent également à l'utilisation des systèmes d'information extérieurs à l'université accessibles via les moyens informatiques de l'établissement.

Engagements de l'université

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

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

L'université facilite l'accès des utilisateurs aux ressources du système d'information dont l'usage est nécessaire à l'exercice de leurs fonctions. Les ressources mises à leur disposition sont principalement à usage professionnel.

Engagements 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, de discrétion 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.

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

2. Droits d'accès au système d'information

L'accès au système d'information (ressources informatiques, service Internet, réseau, ...), est accordé à toute personne autorisée par l'université jusqu'à échéance de son autorisation (fin de contrat, mutation, retraite, etc.)

Ce droit est personnel et ne peut être cédé même temporairement à un tiers, il est matérialisé par la création d'identifiants nominatifs et confidentiels (couple nom d'utilisateur / mot de passe).

Un utilisateur ne peut en aucun cas permettre à une autre personne, d'accéder au système d'information (SI) de l'université au moyen de ses identifiants. Dans cette situation l'utilisateur sera responsable des actions effectuées avec ses identifiants.

3. Conditions d'utilisation du système d'information et des ressources informatiques

Les moyens et systèmes informatiques de l'université de Toulon incluent notamment les serveurs, les stations de travail et les micro-ordinateurs des bureaux, des salles de cours ou informatiques et des salles de laboratoires (qu'ils soient ou non connectés au réseau), les routeurs, les commutateurs, les points d'accès Wi-Fi, les câbles et les fibres optiques, et plus généralement tout équipement électronique appartenant à l'université ou un de ses partenaires (notamment le CROUS) permettant l'échange ou le transfert d'information sous format numérique.

3.1 Utilisation professionnelle / privée

Les ressources mises à disposition de l'utilisateur doivent être utilisées exclusivement à des fins professionnelles, pédagogiques, de recherche et d'insertion professionnelle.

Elles peuvent néanmoins, à titre résiduel, être utilisées à des fins privées sous réserve que cette utilisation soit licite, non lucrative, 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.

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 à cet effet ou en mentionnant le caractère privé sur la ressource.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou de l'université de Toulon, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'université ne pouvant être engagée quant à la conservation de cet espace. Les mesures de conservation des données professionnelles sont définies avec le responsable.

L'utilisation du système d'information à titre privé doit respecter la réglementation en vigueur. En particulier, la consultation, détention, diffusion et exportation d'images à caractère pédophile, ou la diffusion de contenus à caractère raciste ou antisémite est totalement interdite.

Il doit être fait un usage raisonnable de toutes les ressources partagées : espace disque, bande passante sur le réseau, occupation des postes de travail, puissance de calcul, logiciels à jetons, etc. En outre les espaces de stockage mis à disposition n'ont pas vocation à contenir des films, de la musique, et des jeux qui ne seraient pas utilisés dans le cadre des missions de l'université.

L'utilisation d'équipements ou de logiciels non fournis par l'université de Toulon engage la responsabilité de l'utilisateur et ne peut être tolérée que si :

- le rapport avec l'activité professionnelle est effectif ;
- la légalité de l'utilisation est incontestable ;
- la disponibilité, l'intégrité et la confidentialité du système d'information sont préservées.

De surcroît :

- la responsabilité de l'université de Toulon ne pourrait être engagée pour des dommages portés à des matériels n'étant pas de sa propriété (typiquement des matériels personnels) lors de leur utilisation sur son réseau ;
- aucune assistance ne sera apportée par les services techniques de l'université pour la configuration des matériels n'étant pas de sa propriété.

3.2 Continuité de service : gestion des absences et des départs

Il appartient à l'utilisateur de suivre les recommandations de l'autorité hiérarchique (usage des espaces partagés et alias de messagerie) concernant l'accessibilité des données liées à son activité professionnelle. Aux seules fins d'assurer la continuité de service, l'utilisateur veillera, notamment à ce que celles-ci soient accessibles à son supérieur hiérarchique, en cas de départ ou d'absence.

Dans le cas d'un départ ou d'une absence, si les données numériques, à caractère professionnel, n'étaient pas accessibles, le président ou son représentant pourra mandater le directeur de la DSIUN ou son représentant afin que celui-ci accède aux données de l'utilisateur et les transmette au supérieur hiérarchique de l'agent, sous le contrôle du Correspondant Informatique et Liberté de l'université de Toulon après saisine du service juridique de l'établissement. Le service juridique tentera par tous les moyens disponibles de contacter l'utilisateur avant l'intervention. A l'issue de ladite intervention, un rapport circonstancié des actions faites sur le poste sera communiqué à l'utilisateur.

3.3 Règles d'utilisation des ressources informatiques

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information de l'université de Toulon.

L'utilisateur signataire de la présente charte s'engage à respecter les règles ci-dessous et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences de perturber le bon fonctionnement des ressources informatiques et des réseaux.

L'utilisateur s'engage notamment à :

- se conformer aux dispositifs mis en place par l'université de Toulon pour lutter contre les virus et les attaques par programmes informatiques ;
- ne pas utiliser les ressources de l'université pour tenir des propos (oraux ou écrits) qui constituent des infractions au sens de la loi du 29 juillet 1881 sur la liberté de la presse, notamment des propos à caractère insultants, injurieux, diffamatoires, racistes, pornographiques, pédophiles ou attentatoires au respect d'autrui. L'utilisateur est fermement encouragé à respecter les règles de politesse d'usage. Ces règles sont applicables quel que soit le média utilisé (forums, messagerie électronique, dialogue en direct, ...), et quel que soit le destinataire (enseignant, personnel, étudiant) ;
- ne pas porter atteinte à l'intégrité d'autres sites ou systèmes qu'ils soient ou non connectés au réseau ;
- respecter la gestion des accès, en particulier ne pas utiliser les identifiants d'un autre utilisateur, ni chercher à les connaître ;
- ne pas tenter d'accéder à des ressources du système d'information et aux communications entre tiers, pour lesquelles il n'a pas reçu d'habilitation explicite, notamment en :
 - usurpant l'identité d'une autre personne ;
 - s'appropriant le mot de passe d'un autre utilisateur ;
 - se connectant sur un site en accès limité sans y être autorisé ;
 - dissimulant sa véritable identité ;
 - accédant à des informations appartenant à d'autres utilisateurs du réseau sans autorisation.
- ne pas modifier ou détruire des informations dont il ne serait pas propriétaire ;
- ne pas rendre accessibles à des tiers les services qui lui sont offerts, en particulier les moyens d'accès et d'identification (tels que l'adresse électronique, la clé, la carte magnétique, le code et le mot de passe) sont personnels et ne doivent en aucun cas être cédés ;
- ne pas nuire volontairement au bon fonctionnement du système d'information et des réseaux ou à l'activité d'un tiers par des manipulations anormales des matériels ou par l'introduction volontaire de logiciels malveillants (virus, chevaux de Troie, bombes logiques...)

- ne pas connecter directement aux réseaux locaux des matériels sans prévenir au préalable le service technique en charge du réseau ;
- ne pas installer, télécharger ou utiliser sur le matériel de l'université de Toulon, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance ;
- ne pas conserver et à supprimer de ses équipements personnels les logiciels dont la licence d'utilisation est accordée à l'université ou à ses membres, dès lors que le contrat le liant à l'université est échu ;
- ne pas développer, installer ou copier un programme pour contourner la sécurité ou saturer les ressources informatiques ;
- ne pas introduire d'outils d'intrusion et effectuer des tests de sécurité sur le système d'information sans autorisation préalable ;
- ne pas utiliser les ressources mise à sa disposition pour un usage commercial à titre privé. En particulier l'accès aux ressources électroniques fournis par les bibliothèques universitaires doit se faire dans le cadre des droits accordés par l'éditeur.

Toute utilisation d'outils ou services externes tels que Dropbox, Google docs, Google Forms, Google Agenda, Gmail, etc qui conduisent à faire transiter ou à déposer des informations professionnelles et/ou pédagogiques hors des supports et des services offert par l'université engage la responsabilité de celui qui les utilise. En effet, ces pratiques présentent un risque de vulnérabilité particulier du point de vue, d'une part, de la confidentialité des données, d'autre part de la protection du patrimoine scientifique, technique et littéraire mais également des libertés individuelles.

4 Communication électronique

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'université.

(a) Adresses électroniques

L'université de Toulon 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 relève de la responsabilité de l'utilisateur.

L'usage des adresses institutionnelles de type prenom.nom@univ-tln.fr doit être privilégié dans tout échange.

Les informations émanant de l'administration et véhiculées par le biais du courriel, seront communiquées aux utilisateurs exclusivement sur leur adresse électronique institutionnelle.

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'université.

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'université : ces listes ne peuvent être utilisées sans autorisation explicite. L'utilisation de ces listes est soumise à une charte spécifique disponible sur le site intranet de l'université.

L'usage d'adresse électronique non professionnelle engage la responsabilité de l'utilisateur en cas de diffusion à des tiers, même involontaire, de données personnelles, confidentielles, ou soumises à l'obligation de discrétion.

(b) Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé 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 : dans ce cas, les termes en sont précisés et portés à la connaissance de l'utilisateur par la DSIUN.

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...).

L'utilisation de la messagerie professionnelle par les organisations syndicales depuis les systèmes d'information de l'université est régie par un texte spécifique.

(c) Émission et réception 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 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, sur le plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 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.

4.2 Internet

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

L'utilisation d'Internet (par extension l'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'université.

Internet est un outil de travail ouvert à des usages professionnels correspondant aux missions de l'université. Si une utilisation résiduelle privée, telle que définie au point 3.1, peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique ou aux réseaux mis à disposition par l'université de Toulon sont présumées avoir un caractère professionnel. L'université de Toulon peut les rechercher afin de les identifier.

L'université 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'université de Toulon.

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.

Tout téléchargement de fichiers, notamment de sons, d'images ou de vidéos, sur Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis au point 5.1.

L'université de Toulon se réserve le droit de limiter le téléchargement de certains fichiers pouvant présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information, codes malveillants, programmes espions, etc.).

5. Conformité aux règlements et lois en vigueur

5.1 Respect de la propriété intellectuelle

L'université rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et, plus généralement, de tout tiers titulaires de tels droits.

En conséquence, chaque utilisateur se doit :

- d'utiliser les logiciels dans les conditions des licences afférentes ;
- de ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies, sons, 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 ;
- de respecter le droit des marques.

5.2 Respect de la loi « informatique et libertés »

L'utilisateur est informé de la nécessité 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 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.

Une donnée est à caractère personnel dès lors qu'elle permet d'identifier de manière directe ou indirecte des personnes physiques.

Constitue un traitement toute opération ou tout ensemble d'opérations portant sur des informations, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Dès lors, tout projet de traitement de données à caractère personnel à l'initiative d'un ou plusieurs utilisateurs, à des fins pédagogiques ou non, doit être réalisé sous la responsabilité d'un personnel de l'UTLN, qui en informe préalablement à sa mise en œuvre le correspondant informatique et libertés (CIL) désigné par l'université de Toulon.

Par ailleurs, conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des Systèmes d'Information.

Ce droit s'exerce auprès du Correspondant Informatique et Libertés (CIL) de l'université de Toulon.

5.3 Respect de la législation concernant le droit à la vie privée

Le droit à la vie privée, le droit à l'image et le droit de représentation impliquent qu'aucune image ou information relative à la vie privée d'autrui ne doit être mise en ligne sans l'autorisation de la personne intéressée.

5.4 Respect des lois concernant la diffusion de l'information

L'utilisation des moyens informatiques mis à disposition par l'université de Toulon doit respecter la réglementation en vigueur. En particulier l'accès, la détention, la diffusion et l'exploitation d'image à caractère pédophile ou la diffusion de messages diffamatoires ou injurieux, les provocations et apologies punies et la publication d'informations confidentielles sont strictement interdits.

6. Règles de sécurité

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

Les identifiants fournis à chaque utilisateur 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.

Tout utilisateur a la charge, à son niveau, de contribuer à la sécurité générale du système d'information, il doit :

- appliquer et respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe :
 - il doit :
 - choisir un mot de passe non trivial composé de lettres majuscules et minuscules, de chiffres et de caractères spéciaux afin d'être difficilement devinable ;
 - garder strictement confidentiels son (ou ses) identifiants et ne pas le(s) dévoiler à un tiers (y compris aux personnels de la DSIUN) ;
 - modifier son mot de passe en cas de doute. En cas de compromission manifeste du mot de passe, la DSIUN de l'université se réserve le droit de suspendre temporairement le compte jusqu'au règlement du problème rencontré ;
 - ne pas quitter son poste de travail (ni ceux en libre-service) en laissant des ressources ou services accessibles et penser à se déconnecter ou à verrouiller la session.
 - il est invité à :
 - utiliser des mots de passe différents pour accéder à des environnements différents (sites universitaires, sites commerciaux, réseaux sociaux, etc.) modifier ses mots de passe à minima une fois par an.
- assurer la protection des informations sensibles (pour lesquelles a été identifié un besoin direct ou indirect de confidentialité) :
 - protéger ses données en effectuant régulièrement des sauvegardes ;
 - protéger ses fichiers et données contre la lecture et l'écriture en utilisant tous les moyens mis à leur disposition par le système d'exploitation utilisé ;
 - éviter de les transporter sans protection sur des supports non fiabilisés (clés USB, ordinateurs portables, disques externes, etc.) ne pas les déposer sur un serveur externe et/ou ouvert au grand public.
- avertir la DSIUN par mail (dsiun@univ-tln.fr) dans les meilleurs délais de tout dysfonctionnement constaté ou de découverte d'anomalies affectant la sécurité du système d'information, tel un accès frauduleux et notamment l'utilisation illicite de son propre compte. Il signale également toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

6.2 Unités mixtes de recherche et spécificité défense

Certaines UMR peuvent être amenées à respecter les chartes et politiques de sécurité de leurs tutelles, dans cette hypothèse elles sont tenues de les communiquer à l'université.

7. Mesures de contrôle de la sécurité et journalisation des accès

L'utilisateur est informé que :

- l'université de Toulon se réserve la possibilité de réaliser des interventions sur les ressources informatiques mises à la disposition des utilisateurs pour effectuer la maintenance corrective, curative ou évolutive en annonçant à l'avance ces interventions dans la mesure du possible ;
- toute information qui pourrait s'avérer bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée et le cas échéant supprimée ;
- l'université de Toulon se réserve la possibilité de réaliser des audits de robustesse des mots de passe des utilisateurs ;
- les infrastructures informatiques de l'université de Toulon peuvent 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 réglementation applicable ;
- l'université de Toulon se réserve le droit de procéder à des contrôles techniques de son infrastructure en mettant en œuvre des outils de traçabilité dans le respect de la réglementation en vigueur ;
- l'université de Toulon est dans l'obligation légale de mettre en place un système de journalisation des accès à ses serveurs et d'un certain nombre d'échanges de données, préalablement à cette mise en place, elle procédera, auprès de la Commission Nationale de l'Informatique et des Libertés, à une déclaration, qui mentionnera notamment la durée de conservation des traces et durées de connexions, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n° 78-17 du 6 janvier 1978 modifiée ;
- les personnels chargés des opérations de contrôle du système 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. Sous réserve du respect dû au secret des correspondances à caractère personnel et à la vie privée de l'utilisateur, ils doivent communiquer à leur hiérarchie toutes informations susceptibles de compromettre le bon fonctionnement technique des applications ou leur sécurité, ainsi que les utilisations ne respectant pas la présente charte et la réglementation en vigueur.

8. Limitation des usages et sanctions des abus

Le non-respect des règles énoncées dans la présente charte pourra donner lieu, indépendamment à d'éventuelles actions civiles et/ou pénales, à la suspension temporaire de l'accès au système d'information de l'université ainsi qu'à d'éventuelles poursuites disciplinaires internes.

9. Opposabilité et entrée en vigueur de la charte

La présente charte annule et remplace tout autre acte ou charte afférent à l'utilisation des ressources informatiques de l'université de Toulon.

Elle est annexée au règlement intérieur de l'université et portée à la connaissance des utilisateurs visés par l'article 1 de la présente charte.

Elle entre en vigueur dès son approbation par le CA de l'université.