

# Charte de bon usage du Système d'Information à l'attention des étudiants 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.

Le terme **utilisateur** désigne la personne agissant sur le système d'information, ici tout étudiant régulièrement inscrit à l'université de Toulon.

La présente charte a pour objet de définir les règles d'usage et de sécurité du Système d'information que l'université de Toulon met à la disposition de ses étudiants.

Ces règles s'étendent également à l'utilisation des systèmes d'informations extérieurs à l'Université accessibles via les réseaux de l'établissement et notamment Internet.

## 2. Droits d'accès au système d'information

L'accès au système d'information (ressources informatiques, service Internet, réseau, ...), est accordé de droit à tout étudiant dûment inscrit pour l'année universitaire en cours :

- Il est maintenu un an après la dernière inscription
- Il est ensuite suspendu pour une durée d'un an
- Il est ensuite supprimé ainsi que toutes les données laissées par l'utilisateur sur les serveurs de l'université soit deux ans après la dernière inscription.

Il peut également être limité ou retiré, par mesure conservatoire, si le comportement de l'utilisateur n'est pas en adéquation avec la présente charte.

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 login / 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'établissement incluent notamment les serveurs, les stations de travail et les micro-ordinateurs, 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 pédagogique / privée**

Les ressources mises à disposition des étudiants doivent être utilisées exclusivement à des fins 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 privée (en temps et en coût généré) doit demeurer négligeable par rapport aux usages liés à la formation.

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 des étudiants n'ont pas vocation à contenir des films, de la musique, et des jeux.

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

- le rapport avec les études suivies 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 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 le réseau de l'établissement,
- 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 Règles d'utilisation des ressources informatiques**

Les utilisateurs sont responsables, en tout lieu, de l'usage qu'ils font du système d'information de l'Université de Toulon.

Les utilisateurs signataires de la présente charte s'engagent 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.

Les utilisateurs s'engagent notamment à :

- se conformer aux dispositifs mis en place par l'institution 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 ils ne seraient pas propriétaires,
- ne pas rendre accessibles à des tiers les services qui lui sont offerts dans le cadre de sa formation, 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'institution, 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,
- 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

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 mis en œuvre 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.

### 3.3 Messagerie électronique

L'université de Toulon s'engage à mettre à la disposition de l'utilisateur une boîte à lettres institutionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

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

Les informations inhérentes au cursus (et/ou aux études poursuivies) ainsi qu'aux activités étudiantes ou à caractère plus général d'information sur l'institution, émanant de l'administration et véhiculées par le biais du courriel, seront communiquées aux utilisateurs exclusivement sur leur adresse électronique institutionnelle.

L'utilisation de cette adresse nominative est de la responsabilité de l'utilisateur.

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. L'utilisation de ces listes est soumise à une charte spécifique disponible sur le site intranet de l'établissement.

### 3.4 Internet

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

Son utilisation est ouverte à des usages pédagogiques et de recherche.

Si une utilisation résiduelle privée peut être tolérée, les connexions établies grâce à l'outil informatique ou aux réseaux mis à disposition par l'administration sont présumées avoir un caractère professionnel. L'administration peut les rechercher à des fins d'identification.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'institution.

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 paragraphe 4.1.

L'établissement 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.).

## **4. Conformité aux règlements et lois en vigueur**

### **4.1 Respect de la propriété intellectuelle**

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

Chaque utilisateur se doit :

- d'utiliser les logiciels dans les conditions des licences souscrites,
- 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.

L'étudiant est informé que ses réalisations et/ou travaux universitaires dans le cadre de sa formation, mémoire, thèse, ... peuvent faire l'objet d'un contrôle anti-plagiat par tout moyen, notamment par l'usage d'applications et/ou logiciels spécifiques.

### **4.2 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 enseignant de l'UTLN, qui en informe préalablement à sa mise en œuvre le correspondant informatique et libertés (CIL) désigné par l'établissement.

Par ailleurs, conformément aux dispositions de cette loi, chaque usager 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'établissement.

### **4.3 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.

### **4.4 Respect des lois concernant la diffusion de l'information**

L'utilisation des moyens informatiques mis à disposition par l'établissement 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 (crimes, racisme, négationnisme, crimes de guerre, etc.) et la publication d'informations confidentielles sont strictement interdits.

## **5. 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.

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, les services techniques de l'université se réservent 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 universitaire, 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](mailto: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.

## 6. 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 mises à la disposition des utilisateurs pour effectuer la maintenance corrective, curative ou évolutive en les annonçant à l'avance 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 législation applicable,
- 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. Elle se réserve le droit de mettre en place des outils de traçabilité sur son infrastructure et de procéder à des contrôles techniques dans le respect des lois en vigueur. 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. En revanche, ils doivent communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité, ou si elles ne respectent pas la présente charte et les lois en vigueur.

## **7. Limitation des usages et sanctions des abus**

Le non-respect des règles énoncées dans la présente charte pourra donner lieu, indépendamment à d'éventuelles sanctions civiles et/ou pénales, à la suspension temporaire ou définitive de l'accès aux ressources informatiques de l'Université ainsi qu'à d'éventuelles sanctions disciplinaires internes.

## **8. Entrée en vigueur de la charte**

Le présent document annule et remplace tout autre document ou charte afférent à l'utilisation des ressources informatiques de l'Université de Toulon.

La présente charte a été adoptée par la Commission Formation et Vie Universitaire de l'université de Toulon le .....

Elle est annexée au règlement intérieur de l'Université et portée à la connaissance des utilisateurs. Tout utilisateur l'accepte expressément lors de son inscription..