Charte informatique de l'Université de Toulouse II - Le Mirail à l'usage des étudiants

Ce texte est avant tout un code de bonne conduite mais il a valeur de règlement Intérieur. Il a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation afin d'instaurer un usage correct des ressources informatiques et des services Internet, avec des **règles minimales de courtoisie et de respect d'autrui**.

CHAPITRE 1 L'ACCES AU SYSTEME D'INFORMATION

Article 1 : **Définition de l'utilisateur**

L'utilisateur est le titulaire d'un compte d'accès tel que défini à l'article 3. Il s'agit en l'occurrence des étudiants inscrits à l'université Toulouse II - Le Mirail (UTM)

Article 2 : **Définition du gestionnaire du système d'information**

Le responsable du système d'information de l'UTM est désigné gestionnaire du système d'information. Il peut s'agir de plusieurs services regroupés sous la Direction des Systèmes d'information et de l'informatique (DSII)

Il veille à la protection, à la maintenance, au bon fonctionnement du système d'information et assure le respect de la présente charte par l'ensemble des utilisateurs.

Il assure l'exécution de l'ensemble des formalités et déclarations nécessaires, notamment celles issues de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers, et aux libertés, et de la loi du 10 juillet 1991 sur le secret de la correspondance.

Article 3 : **Compte d'accès**

Un ou plusieurs comptes d'accès sont accordés par la Direction des Systèmes d'information et de l'informatique pour favoriser l'accès à l'information scientifique et pour permettre un partage des connaissances et informations. Ce compte d'accès est au minimum concrétisé par l'octroi d'un nom d'utilisateur et d'un mot de passe strictement personnels et confidentiels après acceptation écrite de la charte par le gestionnaire sur l'un quelconque des équipements de l'UTM utilisateur.

L'utilisateur est informé que les mots de passe 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.

L'utilisateur est responsable des opérations effectuées grâce à son identifiant et son mot de passe ; il ne peut les divulguer ou s'approprier ceux d'un autre utilisateur.

Article 4 : **Disponibilité du service**

L'UTM s'efforce, dans la mesure du possible, de maintenir accessible le service qu'elle propose de manière permanente mais n'est tenue à aucune obligation d'y parvenir.

L'UTM peut interrompre l'accès, notamment pour des raisons de maintenance, de mise à niveau et de sécurité, sans pouvoir être tenue pour responsable des conséquences de ces interruptions tant à l'égard des utilisateurs que des tiers.

Article 5 : **Droits de l'utilisateur**

Le compte d'accès donne à l'utilisateur un droit d'accès annuel aux services mis à disposition. Ce droit d'accès est personnel, incessible et temporaire. Il fait l'objet d'un renouvellement annuel. Il disparaît dès lors que son titulaire ne répond plus aux critères d'attribution définis à l'article 1 de la présente charte.

Ce droit d'accès peut être suspendu à tout moment, dès lors qu'est supposé un manquement aux dispositions de la charte de la part de l'utilisateur.

L'utilisateur peut demander à l'UTM la communication des informations nominatives le concernant et les faire rectifier en application des dispositions de la loin° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et auxlibertés.

Article 6 : **Obligations de l'utilisateur**

L'utilisateur est informé qu'en application des dispositions législatives et réglementaires en vigueur, l'UTM est tenu de recueillir et conserver des informations sur les utilisateurs de ses services informatiques et peut, dans le cadre d'une enquête judiciaire, être dans l'obligation de les donner.

En conséquence, tout refus de l'utilisateur relatif à la collecte des informations à caractère personnel demandées implique le rejet de la demande de compte d'accès.

L'utilisateur s'engage à informer immédiatement le gestionnaire de toute perte, de toute tentative de violation ou anomalie relative à une utilisation de son compte d'accès.

L'utilisateur s'engage à effectuer une utilisation rationnelle et loyale des services et, notamment du réseau, de la messagerie et des ressources informatiques afin d'en éviter la saturation et le détournement à des fins personnelles.

L'utilisateur est averti que l'UTM puisse avoir connaissance des informations nécessaires à l'administration du réseau (données de volumétrie, incidents, nature du trafic engendré) et puisse prendre toutes mesures urgentes pour stopper la perturbation de ses services. L'UTM se réserve, notamment, la possibilité de stopper l'accès aux services en cas d'utilisation excessive ou non conforme à ses missions spécifiques.

L'utilisateur est responsable de l'usage qu'il fait du réseau. Il assure notamment, à son niveau, la sécurité de ce réseau et s'engage à ne pas apporter volontairement de perturbations à son fonctionnement et à mettre en péril l'intégrité des ressources informatiques.

Il s'engage, notamment, à :

• ne pas interrompre le fonctionnement normal du réseau ou des systèmes connectés ;

• ne pas développer, installer ou copier des programmes destinés à contourner la sécurité, saturer les ressources ;

• ne pas introduire des programmes malveillants ou contournant la protection des logiciels ;

• ne pas installer de logiciels susceptibles de modifier la configuration des machines sans accord préalable du gestionnaire ;

• ne pas s'attaquer aux systèmes d'information de l'UTM ou de tout autre organisme public ou privé, européen ou étranger, en modifier ou altérer le contenu ;

• ne pas collecter ou tenter de collecter des informations susceptibles d'être utilisées lors de tentatives d'attaques contre des systèmes d'information externes ou internes ;

• ne pas utiliser les ressources informatiques afin de dupliquer, diffuser ou distribuer des logiciels, images, sons et vidéos aux contenus visés par le code pénal ou collectés par des moyens contraires au droit de la propriété intellectuelle, sous quelque forme que ce soit.

L'utilisation à des fins privées doit être non lucrative et raisonnable, tant dans la fréquence que dans la durée. Elle ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

Article 7 : Contrôle et maintenance par le gestionnaire

Les personnels en charge des opérations de contrôle sont soumis au secret professionnel. Ils ne peuvent donc divulguer les informations qu'ils sont amenés à connaitre dans le cadre de leur fonction en particulier lorsque ces informations sont couvertes par les secrets des correspondances ou relèvent de la vie privée de l'utilisateur dès lors que ces informations ne remettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité.

L'utilisateur est averti que le gestionnaire peut avoir accès à l'ensemble des composants du système d'information et ce afin d'effectuer tout acte de protection du système d'information et notamment :

• la conservation et sauvegarde, le contrôle de l'absence de diffusion non autorisée d'informations sur les sites web,

• la preuve de la date de création ou de diffusion des dites informations,

• la recherche et le rejet d'intrusions dans le système d'information ou de matériels violant les règles relatives au droit d'auteur,

• la mise à jour, maintenance, correction et réparation des matériels et logiciels...

Dans le cas où un composant du système d'information ne se trouverait pas dans l'enceinte de l'UTM, l'utilisateur qui en a la garde s'oblige à le restituer ou le confier au gestionnaire à la première demande de sa part.

Le gestionnaire pourra mettre en place des outils de contrôle et de surveillance répondant strictement à la législation en vigueur; et notamment des ressources matérielles et logicielles ainsi que les échanges via le réseau.

A cette fin, l'UTM dispose déjà des moyens techniques suivants pour procéder à des contrôles de l'utilisation de ses services :

• conservation des journaux liés à l'activité informatique,
• pare-feux,
• systèmes de détection d'intrusion,
• serveur de métrologie.

Tout utilisateur peut obtenir auprès du gestionnaire les informations sur les moyens de contrôle mis en oeuvre.

Les contrôles techniques qui peuvent être effectués sont justifiés par un souci de sécurité du réseau *eUou* des ressources informatiques.

La DSII veille au respect des règles en vigueur tant de la part des utilisateurs que des services dépendants du gestionnaire. En particulier , la DSII sera saisie, dès lors que sera soulevé un risque ou constat d'atteinte aux droits des personnes ou aux libertés individuelles qui ne serait pas justifié par la nature de la tâche à accomplir ni proportionné au but recherché.

Les services de la DSII peuvent être amenés à effectuer des sauvegardes, y compris sur les contenus personnels, dans le but exclusif d'empêcher des pertes d'informations. Ces contenus ne sont pas accessibles aux tiers, sauf procédure juridictionnelle.

Article 8 : **Protection contre les programmes malveillants**

L'utilisateur s'engage à ne pas entraver le bon fonctionnement du système de protection mis en place par l'UTM. Seul le gestionnaire est autorisé à introduire dans le système d'information de nouveaux logiciels. En cas de besoin exprimé par un utilisateur pour un nouveau logiciel, il devra demander, à l'administrateur, une autorisation préalable.

La connexion au réseau d'un matériel non référencé par l'UTM n'est envisageable que si le matériel dispose d'outils de protection performants (antivirus, anti spyware, ...). Son utilisation est soumise à autorisation préalable ; l'administrateur vérifie l'efficacité du système de protection.

Le non-respect de ces dispositions peut exposer l'utilisateur à des sanctions et à la mise en jeu de sa responsabilité en cas d'intrusion, du fait de l'utilisateur, de virus ou d'un tiers non autorisé dans le système d'information ou de pertes de données.

Article 9 : **Pare-feux**

L'UTM charge la DSII de définir sa politique de sécurité.

Elle dispose de pare feux (firewall) pour protéger son réseau. Ces équipements ont pour vocation de limiter certains trafics, soit en fonction des protocoles utilisés, soit en fonction des ports, soit en fonction des adresses IP. Le gestionnaire détermine les règles de filtrage à mettre en Œuvre afin de garantir un niveau de sécurité optimal, prenant en compte les règles fixées par la DSII. Tout utilisateur pourra faire une demande écrite et justifiée de modification des règles auprès du gestionnaire. Le gestionnaire pourra alors donner suite si cette demande est conforme à la politique de l'UTM.

CHAPITRE Il UTILISATION DE LA MESSAGERIE ELECTRONIQUE

Article 10 : **Adresse électronique**

Chaque étudiant peut disposer d'une messagerie électronique composée de son prénom et de son nom. En cas d'homonymie, le gestionnaire fixera la règle d'attribution. L'utilisation d'un pseudonyme ou l'usage d'un faux nom est expressément prohibé , sauf autorisation du gestionnaire qui s'assurera du bien-fondé de cette utilisation.

Article 11 : **Utilisation de la messagerie**

L'usage privé de la messagerie (envoi et réception de messages) devra gêner le moins possible le trafic normal, et ce en termes de volume et de taille des messages échangés ainsi que de format des pièces jointes.

Le gestionnaire peut limiter le format, le type et la taille des messages électroniques, y compris des pièces jointes. Les messages non conformes à ces limitations ou comportant un programme malveillant ne seront pas distribués.

Les messages électroniques n'ont pas vocation à être conservés sur le serveur. L'utilisateur qui ne se conformerait pas à un usage raisonnable de sa messagerie en dépassant l'espace de stockage provisoire mis à sa disposition sur le serveur expose le contenu de sa messagerie à la destruction.

L'utilisateur est informé que l'UTM n'exerce aucune surveillance ni aucun contrôle éditorial sur les messages envoyés et reçus. L'UTM ne pourra, de ce fait, être tenu pour responsable de ces contenus .

Article 12 : vie privée

L'utilisateur a droit au respect de sa vie privée; celle-ci implique le secret de ses correspondances et de ses contenus personnels.

L'utilisateur porte l'entière responsabilité des messages personnels transmis par le biais de cette messagerie. Tout usage illicite ou abusif peut entrainer la suppression immédiate de l'accès à la messagerie personnelle.

Par ailleurs, l'utilisateur s'attachera à conserver sur son propre espace de stockage les éventuelles correspondances privées dans un fichier spécifique portant son nom et la mention «correspondance privée ».

CHAPITRE Ill UTILISATION DES SERVICES INTERNET

Article 13 : **Services mis à disposition**

L'UTM offre à l'utilisateur, dans la mesure de ses capacités techniques, l'accès à l'Internet et se réserve d'éventuelles restrictions d'usages.

Article 14: Dispositions législatives et réglementaires

L'utilisateur s'engage à respecter les dispositions législatives et réglementaires en vigueur, notamment

• celles relatives à la propriété littéraire et artistique, contenues, en particulier, dans le code de la propriété intellectuelle. Le téléchargement de logiciels ou d'Œuvres protégés, sans autorisation des ayants droit engage la seule responsabilité de l'utilisateur. L'Administrateur se réserve la possibilité d'effacer du système d'information toute trace de ces logiciels et Œuvres.

• celles relatives à l'informatique, aux fichiers et aux libertés (loi du 6 janvier 1978),

• celles relatives à la protection de la vie privée et du droit à l'image d'autrui.

Par ailleurs, l'utilisateur déclare se soumettre aux règles spécifiques d'utilisation de certaines ressources mises à disposition par l'UTM et pour lesquelles il serait informé de l'existence de conditions contractuelles restrictives liant l'UTM à des tiers, portant en particulier sur l'utilisation d'Œuvres protégées et des ressources documentaires électroniques.

En outre, en application du principe de neutralité commerciale applicable aux établissements publics à caractère scientifique, culturel et professionnel, l'utilisateur s'interdit de faire de la publicité sur des produits et services à caractère commercial.

En application du principe de neutralité politique et religieuse applicable aux établissements publics à caractère scientifique, culturel et professionnel, l'utilisateur s'interdit toute prise de position sur des sujets politiques généraux ne portant pas directement sur les missions de l'université ainsi que toute manifestation de prosélytisme religieux.

L'utilisateur s'interdit de produire, consulter ou télécharger des documents dont le contenu présente un caractère raciste, pornographique, pédophile, injurieux, diffamatoire, incitant à la consommation de substances interdites, à la commission de crimes ou délits, au suicide ou de nature à porter préjudice, de manière générale à l'image de la communauté universitaire.

Le constat par le gestionnaire de manquements à ces obligations par l'utilisateur entraine son exclusion immédiate des services mis à disposition.

Par ailleurs, l'UTM dénoncera tout acte délictueux aux autorités judiciaires, et ce, sans préjudice de l'application de sanctions internes à l'UTM.

Article 15 : **Obligations contractuelles de l'utilisateur**

L'accès à Internet se fait par le réseau RENATER dont la charte s'impose aux utilisateurs. Le réseau RENATER est destiné à véhiculer le trafic engendré par des activités d'enseignement et de recherche. Les autres activités sont par principe prohibées.

L'utilisateur est cependant autorisé à consulter des sites web à titre privé à la condition que cette navigation n'entrave pas l'accès des autres utilisateurs et ne gêne pas la bonne marche du système d'information en raison, en particulier, de l'encombrement de fichiers téléchargés.

Article 16: Environnement Numérique de Travail

L'Environnement numérique de travail (ENT) fonctionne sous la responsabilité informatique du gestionnaire et sous la responsabilité éditoriale du Président de l'UTM.

Aucun utilisateur ne peut introduire un élément dans le site ou modifier des éléments produits par l'UTM sans l'autorisation du gestionnaire. Les utilisateurs pourront formuler toute suggestion à ces derniers quant au contenu ou au fonctionnement de l'ENT.

Article 17 : **Participation à des forums et des services de discussions**

L'utilisateur s'oblige à un usage loyal de ces services en s'interdisant l'emploi d'un pseudonyme.

L'utilisateur ne saurait engager l'UTM du fait de prises de positions ou de diffusions d'informations illicites sur ces services.

Le gestionnaire se réserve le droit de supprimer tout message litigieux, et ce, sans information préalable de l'utilisateur.

CHAPITRE IV SANCTIONS

Article 18: Délits passibles de sanctions pénales

- Atteinte à la personnalité :

  - atteinte à la vie privée (226-1 al.2 ; 226-2 al.2),
  - atteinte à la représentation de la personne (226-8)
  - dénonciation calomnieuse (226-10),
  - atteinte au secret professionnel (226-13),
  - atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques (226-16 à 226-24, issus de la loi du 6 janvier 1978 informatique et libertés).

- Atteinte aux mineurs : 227-23 ; 227-24 et 227-28 (notamment diffusion de messages pornographiques lorsqu'ils sont susceptibles d'être vus par un mineur).

- Crimes et délits contre les biens

  Escroquerie (313-1 et suite)
  Atteinte aux systèmes de traitement automatisé de données (323-1 à 323-7)

- Infractions de presse (loi du 29 juillet 1881, modifiée)

  Provocation aux crimes et délits (art. 23 et 24)
  Apologie des crimes contre l'humanité (art. 24) ;
  Apologie et provocation au terrorisme (art. 24) ;
  Provocation à la haine raciale (art. 24) ;
  "Négationisme" : contestation des crimes contre l'humanité (art. 24 bis) ;
  Diffamation (art. 30, 31 et 32) ;
  Injure (art. 33).

- Infractions au Code de la propriété intellectuelle

  Contrefaçon d'une œuvre de l'esprit (y compris d'un logiciel) (335-2 et 335-3) ;
  Contrefaçon d'un dessin ou d'un modèle (521-4) ;
  Contrefaçon de marque (716-9 et suite).

- Infractions aux règles de la cryptologie (Loi du 29 décembre 1990)

Article 19: Sanctions pénales spécifiques

La loi n°88-19 du 5 janvier 1988 relative à la fraude informatique, dite "loi Godfrain", punit d'un emprisonnement de trois mois à trois ans et d'une amende de 305€ à 76 224€ , quiconque aura, intentionnellement et au mépris des droits d'autrui :

- accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données; entravé ou faussé le fonctionnement d'un système de traitement automatisé de données ;
- introduit des données dans un système de traitement automatique ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission ;
- procédé à la falsification de documents informatisés ;

La tentative des délits est punie des mêmes peines que le délit lui-même.

Article 20 : **Sanctions disciplinaires**

Outre les sanctions pénales, les étudiants encourent, en cas de non-respect des dispositions de la présente convention, des sanctions disciplinaires.

Le droit d'accès peut être définitivement retiré si le manquement est dament constaté par la section disciplinaire.

Les sanctions encourues sont fixées par le décret n• 92-657 du 13 juillet 1992 modifié fixant la procédure disciplinaire dans les établissements publics d'enseignement supérieur.

Article 21 : **Affichage et formalités**

La présente charte sera affichée dès son adoption par le Conseil d'Administration et sera accessible sur l'Internet et l'intranet de l'UTM.