Université de Bretagne Occidentale

Charte d'usage des ressources informatiques à l'Université de Bretagne Occidentale

Dans le cadre de la mission de service public qu'elle remplit, l'Université de Bretagne Occidentale (UBO) assure et facilite l'accès des utilisateurs aux ressources du système d'information. A ce titre, elle est soumise aux règles de bonne utilisation des moyens informatiques. Elle se doit de faire respecter la loi, le règlement, ses engagements contractuels et les règles déontologiques.

Cette charte est avant tout un code de bonne conduite, mais elle précise aussi certaines règles d'usage en vigueur à l'UBO vis-à-vis de l'utilisation des ressources informatiques. Elle a pour objet de préciser la responsabilité de chaque utilisateur, en accord avec la législation, afin d'instaurer un usage correct des ressources informatiques, dans le respect des lois et d'autrui.

Le non-respect de cette charte engage la responsabilité personnelle de l'utilisateur.

I Définitions

On entend par «ressources informatiques» : les postes de travail, les logiciels, les services en ligne (et notamment l'espace numérique de travail, ENT) et les réseaux.

On entend par «utilisateur» : toute personne, quel que soit son statut, appelée à utiliser les ressources informatiques de l'UBO.

On entend par « entité » : toute structure hébergée à l'UBO.

On entend par « Système d'information » : l'ensemble des moyens matériels, logiciels, les applications et réseaux de télécommunication pouvant être mis à disposition de l'utilisateur.

II Application

La présente charte s'applique aux utilisateurs ayant recours aux moyens informatiques de l'Université ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir des réseaux de l'Université.

Nous aviserons les utilisateurs de toute modification de la présente charte, par une publication de celle-ci sur le site internet de l'UBO et par un message d'information diffusé sur les listes officielles de l'UBO.

III Accès aux ressources informatiques.

L'utilisation des ressources informatiques n'est autorisée que dans le cadre des activités liées à la pédagogie, à la recherche, à l'orientation et à l'insertion professionnelle pour les étudiants, et des activités professionnelles pour les personnels.

Pour son accès à l'Internet, l'Université est connectée au réseau RENATER (REseau NAtional de télécommunications pour la Technologie, l'Enseignement et la Recherche). L'utilisation de ce réseau est régie par une "Charte d'usage et de sécurité"[1] que l'établissement s'est engagé à respecter et faire

[1] voir en Annexe.

respecter.

Les activités prévues par les statuts du GIP (Groupement d'Intérêt Public) RENATER sont les suivantes : les activités de recherche ; d'enseignement ; de développement technique ; de transfert de technologie ; de diffusion d'informations scientifiques, techniques et culturelles ; d'expérimentations de nouveaux services présentant un caractère d'innovation technique ; mais également toute activité administrative et de gestion découlant ou accompagnant ces activités.

L'utilisation des ressources informatiques de l'UBO et la connexion d'un équipement sur le réseau sont soumises à autorisation. Cette autorisation est strictement personnelle et incessible. Elle peut être suspendue à tout moment en cas de non-respect de cette charte. Cette autorisation prend fin lors de la cessation de l'activité qui l'a justifiée.

La connexion d'un équipement au réseau de l'Université ne peut être effectuée que par les personnels habilités (contacter les informaticiens de proximité). En ce qui concerne les connexions Wifi, la validation du compte de l'utilisateur lors de l'accès vaut autorisation.

IV Règles d'utilisation, de sécurité et de bon usage

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès.

L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.

En particulier, l'utilisateur:

- doit appliquer les recommandations de sécurité et de bon usage des ressources informatiques auxquelles il a accès, et notamment se conformer aux dispositifs mis en place par l'entité ou la DSI pour lutter contre les virus ;
- doit assurer la protection de ses données ; il est responsable des droits qu'il donne aux autres utilisateurs sur celles-ci ;
- doit signaler à son responsable ou son informaticien de proximité, toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater ;
- doit se renseigner auprès de son informaticien de proximité sur les règles en vigueur pour toute installation de logiciel;
- choisit des moyens d'authentification personnels sûrs, gardés secrets[2] et en aucun cas ne doit les communiquer à des tiers ;
- s'engage à ne pas mettre à la disposition d'utilisateur(s) non autorisé(s) un accès aux systèmes ou aux réseaux, à travers des moyens dont il a l'usage ;
- ne doit pas utiliser ou essayer d'utiliser des comptes d'accès autres que le sien ni masquer sa véritable identité ;
- ne doit pas quitter son poste de travail ni ceux en libre-service en laissant des ressources ou services accessibles ;
- ne doit pas faire d'utilisation abusive des moyens informatiques en terme de consommation de ressource ou d'utilisation de bande passante.
- doit privilégier le dépôt de ses fichiers de travail sur des zones partagées par les membres de son service ou de son équipe, afin d'assurer la continuité de service. Pour les personnels, le responsable devra prévoir le transfert des données professionnelles de l'utilisateur partant, en concertation avec celui-ci.

V Conditions de confidentialité

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations transitant sur le réseau ou détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées.

L'utilisateur s'engage à ne pas déchiffrer des données non détenues par lui-même (mots de passe, données échangées sur le réseau…)

[2] cf annexe II : choisir un bon mot de passe

VI Protection des données à caractère personnel

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 dite « Informatique et Libertés » modifiée par la loi n° 2004/801 du 6 août 2004.

Les données à caractère personnel sont des informations – sous quelque forme que ce soit – qui permettent directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférentes, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi « Informatique et Libertés ».

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement le CIL (Correspondant Informatique et Liberté) ou le service juridique qui prendront les mesures nécessaires au respect des dispositions légales.

Pour rappel:

- le droit à la vie privée, le droit à l'image et le droit à la représentation impliquent qu'aucune image ou information relative à la vie privée ne soit mis en ligne sans consentement de la personne intéressée.
- le droit à l'accès aux informations personnelles et le droit de rectification : chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant.
- le droit à l'oubli :chaque utilisateur dispose d'un droit de retrait de certaines informations qui pourraient lui nuire sur des actions qu'il a faites dans le passé.
- le droit d'opposition : chaque utilisateur dispose d'un droit de s'opposer à ce que les données le concernant soient diffusées, transmises ou conservées.

VII Respect de la propriété intellectuelle

L'utilisateur ne doit pas reproduire, télécharger, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

Ces dispositions s'appliquent tout particulièrement à l'utilisation des ressources documentaires électroniques du Service Commun de Documentation.[3]

L'utilisateur n'installe pas, ne télécharge pas ou n'utilise pas, sur le matériel informatique de l'UBO, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés.

VIII Préservation de l'intégrité des systèmes informatiques

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales de matériel ou de logiciels.

Il 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 des programmes nuisibles (virus, cheval de Troie, ver...) ;

L'utilisateur contribue à son niveau à la sécurité des systèmes d'information. A ce titre, il fait preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes, hameçonnage, ...).

[3] voir en Annexe.

IX Usage des services en ligne

L'utilisateur doit faire usage des services en ligne dans le cadre exclusif de ses activités professionnelles ou d'études dans le respect de la législation en vigueur.

En particulier :

- il ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités ;
- il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
- il ne doit pas usurper l'identité d'une autre personne ;
- il ne doit pas intercepter de communications entre tiers et il a l'obligation de s'abstenir de toute ingérence dans la transmission des messages en vertu du secret des correspondances privées ;
- il ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- il doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques de toute nature;
- il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à l'Université ;
- il doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère illicite, injurieux, raciste, pornographique, diffamatoire, ainsi que le respect des principes de neutralité religieuse, politique et commerciale.

L'Université ne pourra être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé à ces règles.

X Adresse électronique

L'UBO 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 se fait sous la responsabilité de l'utilisateur.

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'utilisateur utilise ses coordonnées professionnelles, en particulier son adresse électronique ou autre identifiant, avec précaution. En les utilisant sur des sites sans rapport avec son activité professionnelle il facilite les atteintes à sa réputation, à la réputation de l'UBO.

L'utilisateur doit privilégier la boîte à lettre électronique professionnelle lors de l'émission de courriels professionnels.

XI Publication d'informations sur Internet

Toute publication d'information sur les sites internet ou intranet de l'UBO est réalisée sous la responsabilité d'un responsable de site web ou responsable de publication nommément désigné.

Aucune publication d'information à caractère privé (pages privées au sens non professionnelles) sur les ressources du système d'information de l'UBO n'est autorisée, sauf disposition particulière décidée au sein de l'UBO.

XII Informatique en nuage

L'utilisation de service de stockage en ligne et de services hébergés en dehors de l'Université pose de nombreux risques en terme de sécurité pour les informations (disponibilité, confidentialité…).

L'utilisateur s'engage à privilégier pour ces types de service les outils validés et proposés par l'UBO.

L'usage de services de « Cloud computing » (informatique en nuage) externes à l'UBO est toléré. Toutefois, il est primordial que les données sensibles (données dont la diffusion peut porter préjudice) du système d'information ne sortent pas du périmètre maîtrisé par l'UBO.

Selon la criticité des données l'usage pourra être interdit ou nécessiter un chiffrement obligatoire. Se rapprocher du Responsable Sécurité des Systèmes d'Information (RSSI) de l'UBO pour définir les mesures à adopter.

XIII Utilisation personnelle des ressources informatiques

Si une utilisation résiduelle privée peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'UBO sont présumées avoir un caractère professionnel.

Les ressources informatiques fournies à l'utilisateur par l'UBO (poste de travail, serveurs, applications, messagerie, Internet, téléphone, etc.) sont réservées à l'exercice de son activité professionnelle.

Un usage personnel de ces ressources est toutefois toléré à condition :

- qu'il n'affecte pas l'usage professionnel ;
- qu'il ne mette pas en danger leur bon fonctionnement et leur sécurité ;
- qu'il n'enfreigne pas la loi, les règlements et les dispositions internes.

Toute donnée est réputée professionnelle à l'exception des données explicitement désignées par l'utilisateur comme ayant un caractère privé.

Pour la messagerie, il faut mentionner « privé » dans le champ « objet » des messages électroniques.

De même le stockage des données à caractère privé doit se faire en mentionnant le caractère privé sur la ressource utilisée (dans un répertoire nommé "privé").

Cet espace ne doit pas contenir de données à caractère professionnel et il ne doit pas occuper une part excessive des ressources. La protection et la sauvegarde régulière des données à caractère privé incombent à l'utilisateur.

L'utilisateur est responsable de son espace de données à caractère privé et il lui appartient de le détruire au moment de son départ. En cas de circonstances exceptionnelles (départ impromptu ou décès) l'UBO ne conserve les espaces de données à caractère privé présents sur les ressources informatiques fournies par l'UBO que pour une période limitée arrêtée par le Président de l'université (délai permettant à l'utilisateur ou des ayants droits de récupérer les informations qui s'y trouvent).

En tout état de cause les données non situées dans un répertoire "privé" sont considérées comme professionnelles et restent à la disposition de l'employeur.

XIV Devoirs de signalement et d'information

L'utilisateur doit avertir son informaticien de proximité dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, suspicion d'une usurpation d'un code d'accès, etc.

De même, l'utilisateur doit signaler le plus rapidement possible à son informaticien de proximité toute perte ou tout vol d'un équipement mis à sa disposition.

Pour prévenir les vols, l'utilisateur s'engage à utiliser les moyens de protection disponibles (câble antivol, rangement dans un tiroir ou une armoire fermant à clé, etc.) pour garantir la protection des équipements mobiles et des informations qu'ils renferment (ordinateur portable, clé USB, ordiphone, tablette, etc.).

L'informaticien de proximité remontera au Responsable Sécurité des Systèmes d'Information de l'UBO les

informations signalées.

XV Manipulation de données à caractère sensible

L'utilisateur protège les données qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité.

Par données à caractère sensible, il faut entendre les données dont le maintien du secret présente un intérêt digne de protection, en particulier les informations relatives aux données à caractère personnel, à la garantie de la propriété intellectuelle (dépôt de brevet, secret industriel...).

Dans le cadre de la manipulation de données à caractère sensible, il convient d'être vigilant lors de l'utilisation des outils et des réseaux informatiques. En particulier, ces données ne doivent pas circuler en clair sur le réseau , elles ne doivent être accessibles que par les personnes habilitées, elles doivent être chiffrées si possible. Contactez le Responsable Sécurité des Systèmes d'Information pour vous fournir une analyse et des conseils sur les outils adaptés.

Lorsqu'il crée un document, l'utilisateur détermine son niveau de sensibilité et applique les règles permettant de garantir sa protection durant tout son cycle de vie (marquage, stockage, transmission, impression, suppression, etc.).

Afin de se prémunir contre les risques de vol de documents sensibles, l'utilisateur, lorsqu'il s'absente de son bureau, s'assure que ses documents papier, lorsqu'ils existent, sont mis en sécurité et que son poste de travail est verrouillé.

XVI Matériel personnel

Les ressources informatiques personnelles (ordinateurs, smartphones, tablettes, etc. achetés à titre personnel), lorsqu'elles sont utilisées pour accéder aux Systèmes d'Information de l'UBO, 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 protège les équipements personnels qu'il utilise :

- pour accéder, à distance ou à partir du réseau local au Système d'Information de l'UBO;
- pour stocker des données professionnelles;

en respectant les règles édictées par l'UBO.

L'UBO informe l'utilisateur et l'accompagne dans la mise en œuvre de ses mesures de protection.

L'utilisateur n'introduit pas des supports de données (clé USB, CDROM, DVD, etc.) sans respecter les règles de l'UBO et prend les précautions nécessaires pour s'assurer de leur innocuité ;

XVII Analyse et contrôle de l'utilisation des ressources

L'utilisation des ressources informatiques et du réseau peut donner lieu à surveillance et contrôle à des fins de statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus[4] (utilisation d'outils de métrologie, de filtrage, de scan, de détection de vulnérabilité, de détection d'intrusion, de fichiers de journalisation, d'antivirus, d'anti-spam...).

Ces analyses et contrôles se font dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés, exclusivement par les personnels habilités[5] .

La fourniture d'un accès Internet dans le cadre professionnel oblige légalement à mettre en place un système de journalisation pour conserver les données techniques de connexion (loi du 15 nov. 2001 ; décret d'application du 24 mars 2006).

Les personnels habilités pour réaliser ces tâches d'administration sont soumis au secret professionnel. Ils ne

[4] voir en annexe : Politique de gestion des journaux informatiques
[5] voir annexe III : Analyse et contrôle de l'utilisation des ressources

peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

XVIII Mesures prises en cas de non respect de la charte

En cas de manquement aux règles et obligations définies dans cette charte, la Direction des Systèmes d'Information (DSI) de l'UBO :

- interdit temporairement, à titre conservatoire l'accès aux ressources informatiques à un utilisateur qui ne respecte pas la présente charte,
- saisit l'autorité hiérarchique en cas de manquements graves résultant du non-respect de cette charte pouvant déclencher des procédures disciplinaires ou pénales.

Annexe

Charte Renater : https://www.renater.fr/IMG/pdf/charte_fr.pdf

Charte d'utilisation des ressources documentaires électroniques :
https://www.univ-brest.fr/S_Commun/Biblio/charte.html

Politique de gestion des journaux informatiques
http://dsi.univ-brest.fr/menu/les-usages/Chartes/

Annexe I : Rappel des lois

Il est rappelé que toute personne sur le sol français doit respecter la législation française y compris dans le domaine de la sécurité informatique .

A. La protection des libertés individuelles

La création de tout fichier contenant des informations nominatives doit faire l'objet d'une demande préalable auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).
La loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et sa loi modificatrice 2004-801 du 6 août 2004 peuvent être trouvées sur le site http://www.legifrance.gouv.fr.

La Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) s'applique plus spécifiquement au traitement des données à caractère personnel dans le secteur des télécommunications.

B. Le respect du droit de propriété

La législation interdit à tout utilisateur de faire des copies de logiciels commerciaux pour quelque usage que ce soit. Les copies de sauvegarde sont les seules exceptions.

La copie d'un logiciel constitue le délit de contrefaçon sanctionné pénalement (code de la propriété intellectuelle). L'auteur d'une contrefaçon engage directement sa responsabilité, il peut être poursuivi devant les tribunaux répressifs et civils; la personne morale qui l'emploie, par exemple un établissement public, peut également être poursuivie.

La Circulaire Rocard du 17 juillet 90 rappelle expressément que « les fonctionnaires auteurs d'actes de contrefaçon de logiciel devront supporter seuls les condamnations pénales encourues, même s'ils n'ont pas agi dans leur intérêt personnel ».

C. Le respect de l'intégrité d'un système informatique

L'utilisateur s'engage à ne pas effectuer d'opérations pouvant nuire au fonctionnement du réseau, à l'intégrité de l'outil informatique et aux relations internes et externes de l'établissement.

La simple accession à un système sans autorisation constitue un délit, même s'il n'en est résulté aucune altération des données ou fonctionnement dudit système. Si de telles altérations sont constatées les sanctions prévues sont doublées.

Il est à souligner que de tels actes (même de simples tentatives) sont susceptibles d'entraîner l'éviction de l'utilisateur de la fonction publique.

La répression des atteintes aux systèmes de traitement automatisé de données est prévue par la loi du 5 janvier 1988 (Loi dite "Godfrain"), dont les dispositions ont été reprises, depuis le premier mars 1994, par les articles 323-1 à 323-7 du Nouveau Code Pénal.

C.1 Article 323-1

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)
(Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004)

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-2

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)
(Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004)

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)
(Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004)

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3-1

(Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004)

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4

(Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004)

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5

Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines

complémentaires suivantes :

1. L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2. L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
3. La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4. La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5. L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6. L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7. L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre. Les peines encourues par les personnes morales sont :

1. L'amende, suivant les modalités prévues par l'article 131-38 ;
2. Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7

(Loi n° 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004)

La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

D. Le respect du secret de la correspondance

Les utilisateurs doivent s'abstenir de toute tentative d'intercepter les communications privées, qu'il s'agisse de courrier électronique ou de dialogue direct.

La loi numéro 91-646 du 10 juillet 1991 stipule dans son article 2 : "Le secret des correspondances émises par la voie des télécommunications est garanti par la loi", sont concernés : le téléphone, le télécopieur, les liaisons informatiques et télématiques.

De lourdes sanctions pénales frappent celui qui porte atteinte au secret de la correspondance (articles 226-15 et 432-9 du nouveau code pénal).

Annexe II : Choisir un bon mot de passe

Pour ceux qui sont pressés :

Un bon mot de passe contient des majuscules, des minuscules, au moins 1 chiffre et au moins un caractère non alphanumérique.

Exemple : ert#Ty4

Il doit faire au minimum 8 caractères.

Pourquoi choisir un bon mot de passe?

Tout d'abord votre mot de passe est personnel et ne doit être divulgué à aucun tiers. Il est aussi personnel que votre numéro de carte bancaire. Pourquoi? Parce qu'il permet de lire votre courrier électronique d'envoyer des messages électroniques sous votre nom, de consulter votre ENT, d'y consulter vos informations personnelles, d'usurper votre identité sur le réseau informatique.

Retenez-le par coeur :

Votre mot de passe doit être difficile à trouver, mais facile à retenir :Ne l'inscrivez nulle part. En particulier, ne le stockez pas dans un fichier électronique (fichier des paramètres de votre client de messagerie,fichier des préférences de votre navigateur favori), et n'activez pas l'option permettant d'enregistrer votre mot de passe.

Ce qu'il faut éviter :

Que votre mot de passe soit votre identifiant! Le mot de passe ne doit pas être un mot concernant une donnée personnelle (votre nom, numéro de téléphone, votre code postal ...) que l'on peut retrouver facilement. Le mot de passe ne doit pas figurer dans un dictionnaire (dictionnaire français, anglais, noms communs, nom propre...)

Choisir un bon mot de passe :

Un bon mot de passe doit faire au moins 8 caractères. Il doit mixer un maximum de caractères différents : majuscules, minuscules,chiffres, caractères spéciaux (#{[\@%?...)
Il ne doit avoir une signification que pour celui qui l'a créé de façon à le retenir facilement.

Voilà, on ne va pas vous proposer de méthode pour construire ce genre de mot de passe. Votre méthode sera la meilleure pour vous, pour que vous reteniez le vôtre.

Annexe III : Analyse et contrôle de l'utilisation des ressources

A. Réseau

L'utilisateur accepte que l'université 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'université se réserve notamment la possibilité de stopper l'accès aux services en cas d'utilisation excessive ou non conforme .

B. Fichiers de journalisation

En vertu de la loi N°2001-1062 du 15 novembre 2001, les données de connexion permettant d'identifier le poste ou l'utilisateur sont conservées et sauvegardées pendant un délai de trois mois, uniquement pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales et dans le seul but de mettre des informations à la disposition de l'autorité judiciaire.

Depuis le 24 mars 2006, le décret n° 2006-358 précise pour les opérateurs de communications électroniques les modalités relatives à la conservation des données des communications électroniques.

C. Messagerie électronique

Dans le cadre des Services Intranet/Internet de l'Établissement, ce dernier met à la disposition de l'Utilisateur un service de messagerie électronique.
L'Établissement n'exerce aucune surveillance ni aucun contrôle éditorial sur les messages envoyés et reçus dans le cadre de la messagerie électronique. L'Utilisateur le reconnaît et l'accepte. L'Établissement ne pourra, de ce fait, être tenu pour responsable des messages échangés.

La DSI se réserve le droit de mettre en place des « quotas » de taille de boîtes à lettres en raison des nécessités imposées pour une bonne gestion des réseaux.

L'utilisateur accepte un contrôle a posteriori de l'utilisation de sa messagerie qui ne pourra porter que sur des indications générales de fréquence, de volume, de taille des messages, du format des pièces jointes, sans qu'il y ait aucun contrôle sur le contenu des messages échangés.

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, constituer une preuve ou un commencement de preuve. L'utilisateur doit en conséquence être vigilant sur la nature des messages électroniques qu'il échange au même titre que les lettres envoyées.

D. Pages Web hébergées sur le serveur de l'Établissement

L'Établissement se réserve le droit de contrôler le contenu de toute page Web hébergée sur ses serveurs en vue de s'assurer du respect des conditions d'utilisation des services énoncées par la présente Charte.
L'Établissement se réserve le droit de suspendre l'usage du service d'hébergement des pages Web par un Utilisateur en cas de non-respect de la Charte et notamment dans l'hypothèse où l'Utilisateur aurait diffusé sur ses pages Web un contenu manifestement illicite.