

Règlement d'usage des ressources informatiques de l'Université de Limoges

Approuvé en Conseil d'Administration le 2 juillet 2010

1	Préambule.....	3
1.1	Terminologie.....	3
1.2	Objet.....	3
1.3	Engagements de l'université.....	4
1.4	Engagements de l'utilisateur.....	4
2	Conditions d'utilisation des ressources informatiques.....	4
2.1	Utilisation professionnelle / privée.....	4
2.1.1	Etudiants.....	4
2.1.2	Personnels de l'université.....	4
2.2	Continuité de service : gestion des absences et des départs.....	5
2.3	Personnes extérieures à l'université.....	5
3	Principes de sécurité.....	5
3.1	Règles générales de sécurité.....	5
3.2	Comptes, mots de passe, autorisations.....	5
3.3	Devoirs de signalement et d'information.....	6
3.4	Installation de logiciels.....	6
4	Rôle des administrateurs des ressources informatiques.....	6
5	Communications électroniques.....	7
5.1	Messagerie électronique.....	7
5.1.1	Adresses électroniques.....	7
5.1.2	Contenu des messages électroniques.....	7
5.1.3	Statut et valeur juridique des messages.....	7
5.1.4	Sécurité.....	8
5.2	Internet.....	8
5.2.1	Accès à Internet.....	8
5.2.2	Publications sur les sites internet et intranet de l'université.....	8
5.2.3	Sécurité.....	8
5.3	Téléchargements.....	9
6	Traçabilité, surveillance et contrôle des ressources informatiques.....	9
6.1	Traces et surveillance.....	9
6.2	Contrôle de la sécurité, maintenance.....	9
6.3	Bilan annuel.....	9
7	Aspects légaux.....	10
7.1	Respect de la propriété intellectuelle.....	10
7.2	Loi « Informatique et Libertés ».....	10
7.2.1	Information sur la loi.....	10
7.2.2	Correspondant « Informatique et Libertés ».....	10
7.3	Respect des personnes, non-discrimination.....	11
7.4	Respect de la vie privée, droit à l'image.....	11
7.5	Atteintes aux systèmes de traitement automatisé de données.....	11
8	Limitations des usages.....	11
9	Entrée en vigueur du règlement.....	11

Note de synthèse

Cette note résume le règlement d'usage des ressources informatiques de l'Université de Limoges. Elle ne s'y substitue pas.

Le système d'information est primordial pour l'accomplissement des missions de l'université, en pédagogie, en recherche, ainsi que dans les activités de pilotage ou administratives. Il s'appuie en grande partie sur des *ressources informatiques*, de nature matérielle (ordinateurs fixes ou nomades, réseaux, téléphonie, ...) ou immatérielle (logiciel, données, ...).

Les usagers disposent, à travers ces ressources, d'outils de communication, favorisant l'enseignement, la recherche, la culture ... Par leurs actions, ils contribuent au bon fonctionnement et à la sécurité du système. Ils doivent être avertis et protégés des risques liés à son utilisation.

Par ailleurs, la législation impose ses propres règles, tout en apportant des éléments de protection pour les personnes.

Dans ce cadre, le règlement d'usage des ressources informatiques a pour objet de définir les droits et les devoirs respectifs des utilisateurs et de l'université.

L'université met en œuvre des moyens de protection des utilisateurs et de leurs données.

L'université a un devoir d'information envers les utilisateurs. Ainsi, il est porté à la connaissance des utilisateurs que des traces, à des fins d'analyse du fonctionnement ou de sécurité, sont enregistrées sur les systèmes. Par ailleurs, les éléments bloquants ou dangereux pour le système peuvent être désactivés ou supprimés (par exemple les virus).

L'université fournit une adresse mél nominative et un accès Internet.

Les utilisateurs ont un droit résiduel à la vie privée. Ils peuvent utiliser les ressources informatiques de manière privée et confidentielle (moyens de communication, de stockage) ; cependant cet usage ne doit pas entraver ou prendre une part conséquente des ressources.

Les données des étudiants sont considérées comme relevant de la vie privée, à l'exception des données partagées à des fins pédagogiques.

Pour les personnels, ce droit ne doit pas nuire au fonctionnement du service. Seules les données relevant clairement de la vie privée jouissent d'une confidentialité. Ainsi, l'accès à un compte peut être débloqué en cas de nécessité.

Les utilisateurs sont responsables de l'usage qu'ils font des ressources qui leur sont confiées. Ils doivent respecter quelques règles, comme préserver la confidentialité des informations auxquelles ils accèdent et les codes d'accès de leur compte. Ils ne doivent pas chercher à contourner les mesures de sécurité, à accéder à des systèmes sans habilitation, à brancher des équipements ou services sur le réseau sans autorisation. Ils doivent respecter la législation en vigueur, par exemple sur le droit d'auteur (pas de copie illicite de logiciels ou d'œuvres), le respect des personnes (diffamation, injure), la déclaration des données nominatives.

Les utilisateurs doivent faire part des anomalies ou incidents portés à leur connaissance. Ils doivent respecter les consignes sur l'utilisation des ressources informatiques.

Le règlement précise enfin le rôle des administrateurs. Pour assurer le bon fonctionnement des ressources informatiques et leur sécurité, ils disposent d'un accès étendu. Ils sont tenus à un devoir de confidentialité quant aux informations auxquelles ils peuvent avoir accès.

En cas de non respect du règlement, des mesures conservatoires pourront être prises, sans préjuger d'autres poursuites.

1 Préambule

Le présent règlement est à destination des utilisateurs des ressources informatiques de l'Université de Limoges. Il donne les règles d'usage et de sécurité s'appliquant à l'université ainsi qu'à l'ensemble des utilisateurs.

1.1 Terminologie

Dans la suite du document, par « université » s'entend l'Université de Limoges.

Par « ressources informatiques », s'entend l'ensemble des données et des systèmes informatiques (réseaux de télécommunications, ressources logicielles ou matérielles, y compris nomades tels que assistants personnels, ordinateurs portables, téléphones portables, ...), pouvant être mis à disposition par l'université¹.

Par « entité », s'entend tout service, laboratoire, institut, faculté, école, etc. faisant partie de l'université.

Par « utilisateur », s'entend toute personne ayant accès, dans le cadre de l'exercice de son activité, aux ressources informatiques, quel que soit son statut. Ainsi sont notamment désignés :

- les usagers du service public d'enseignement² ;
- les personnels d'enseignement et de recherche, titulaires ou non, permanents ou invités ;
- tout agent (administratif, technique ...) titulaire ou non titulaire concourant à l'exécution des missions de l'université ;
- toute personne faisant partie d'un organisme, d'une entreprise ou autre hébergé sur les ressources informatiques de l'université, par exemple réseaux, serveurs ou services numériques ;
- tout prestataire ayant contracté avec l'université ou avec une collectivité territoriale ayant compétence partagée avec l'université.

Par « administrateur », s'entend toute personne effectuant des opérations d'installation, de maintenance, d'administration ou de contrôle de tout ou partie des ressources informatiques ; ceci inclut les personnels (ingénieurs, techniciens, enseignants, ...) disposant de droits étendus permettant l'accès à des informations à caractère personnel d'autres utilisateurs (information nominatives, données personnelles, traces, ...).

Par « responsable informatique d'entité », s'entend la personne nommée ou identifiée comme étant en charge des ressources informatiques au sein d'une entité³.

1.2 Objet

Le bon fonctionnement de l'université suppose le respect des règles visant à assurer la sécurité⁴ de ses ressources informatiques, notamment pour la performance des traitements et pour la conservation des données. Il importe aussi que chacun respecte les dispositions législatives et réglementaires qui s'imposent, dans le respect des droits élémentaires.

Ce règlement définit les règles d'usages et de sécurité que l'université et l'utilisateur s'engagent à respecter : il précise les droits et devoirs de chacun.

Il rappelle les principales dispositions législatives en vigueur pour son application. Il peut être

¹ Les moyens nomades personnels, appartenant à des usagers, ne font pas partie du système d'information ; seules leurs modalités d'accès au système d'information et aux réseaux sont couvertes par ce règlement.

² Cf. règlement intérieur de l'université : étudiants en formation initiale ou continue, etc.

³ Un responsable informatique peut être un administrateur ou une personne qui dirige une équipe d'administrateurs.

⁴ Par sécurité, on entend la préservation des critères de confidentialité, intégrité, disponibilité.

complété par des guides d'utilisation définissant les principales règles pratiques d'usage.

1.3 Engagements de l'université

L'université facilite l'accès des utilisateurs aux ressources informatiques. Elles sont mises à leur disposition pour répondre aux missions de l'université, dans le respect de la vie privée, des libertés individuelles et universitaires de chacun.

L'université porte à la connaissance de l'utilisateur le présent règlement.

L'université met en œuvre toutes les mesures nécessaires pour assurer la sécurité des ressources informatiques et la protection des utilisateurs, dans le respect des droits fondamentaux.

1.4 Engagements de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait des ressources informatiques auxquelles il a accès, ou mises à sa disposition par l'université.

Il a une obligation de réserve 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 déontologie⁵.

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

2 Conditions d'utilisation des ressources informatiques

2.1 Utilisation professionnelle / privée

Les ressources mises à disposition des utilisateurs sont des outils de travail ouverts à des usages professionnel, pédagogique, de recherche et administratif, et peuvent constituer le support d'un usage privé.

L'utilisation résiduelle à titre privé doit être non lucrative et raisonnable, autant dans sa fréquence, sa durée, que sa quantité. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

2.1.1 Etudiants

Par défaut, toute information contenue dans le compte nominatif attribué individuellement, sera considérée comme relevant de la vie privée.

Des espaces de partage documentaire, ou des comptes spéciaux, prévus à des fins pédagogiques, peuvent être créés. Ils ne seront pas considérés comme privés, les conditions d'utilisation et d'accès seront précisées aux étudiants par le responsable pédagogique.

2.1.2 Personnels de l'université

L'utilisation à usage privé ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre, au bon fonctionnement du service ou à l'accomplissement des missions de l'université.

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 explicitement⁶ à cet effet. La sauvegarde des données à caractère privé incombera à l'utilisateur.

⁵ Notamment le secret médical dans le domaine de la santé

⁶ Par exemple, cet espace pourrait être nommé Perso, _privé_

2.2 Continuité de service : gestion des absences et des départs

Cette section ne concerne pas les étudiants.

En cas d'absence non planifiée et pour des raisons exceptionnelles, si un utilisateur se trouve dans la nécessité de communiquer ses codes d'accès⁷ aux ressources informatiques, il doit procéder, dès que possible, au changement de ces derniers ou en demander la modification à l'administrateur.

En cas de force majeure, et à la seule fin d'assurer la continuité du service, un administrateur peut ouvrir, sous la responsabilité du supérieur hiérarchique, l'accès à un compte, en préservant la confidentialité des données à caractère privé.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif de son entité ou de l'université, 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 et transmission des données professionnelles sont définies avec le responsable informatique d'entité ou avec l'université.

2.3 Personnes extérieures à l'université

Toute personne hébergée par l'université, à titre individuel ou non⁸, et accédant aux ressources informatiques, devra respecter ce règlement. En conséquence, tout contrat, invitation, convention, etc. devra comporter l'obligation de respect du présent règlement.

3 Principes de sécurité

3.1 Règles générales de sécurité

L'université met en œuvre les mécanismes de protection appropriés sur les ressources informatiques mises à la disposition des utilisateurs.

La sécurité de ces ressources nécessite plusieurs précautions:

- 1) de la part de l'université :
 - a) veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service (Cf. section 2.2) ;
 - b) limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;
- 2) de la part de l'utilisateur :
 - a) s'interdire d'accéder ou de tenter d'accéder à des ressources pour lesquelles il n'a pas reçu d'habilitation explicite ;
 - b) ne pas connecter directement aux réseaux des matériels autres que ceux confiés ou autorisés par l'université ou son entité, dans les conditions spécifiées ;
 - c) se conformer aux dispositifs mis en place par l'université ou son entité pour lutter contre les risques de sécurité.

3.2 Comptes, mots de passe, autorisations

L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité destinée à identifier les accès, à gérer les autorisations, 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 son statut ou de ses missions. La sécurité des ressources informatiques mises à sa disposition lui impose :

⁷ Identifiants, mots de passe, dispositifs d'accès logique ou physique (carte à puce, clés de sécurité ...)

⁸ Stagiaire, chercheur invité, prestataire, organisme, association, entreprise, etc.

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ;
- de garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers (sauf cas prévus en section 2.2) ;
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.

3.3 Devoirs de signalement et d'information

L'université doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation des ressources informatiques. L'université mène des actions de formation et d'information à destination des utilisateurs, pour faciliter l'usage des ressources dans le respect des règles de sécurité.

L'utilisateur doit avertir son entité (responsable informatique ou hiérarchie) ou l'université dans les meilleurs délais de tout dysfonctionnement constaté, ou de toute anomalie ou incident découvert telle une intrusion dans des ressources informatiques. Il signale également toute possibilité d'accès qui ne corresponde pas à son habilitation.

3.4 Installation de logiciels

Certains utilisateurs peuvent avoir des droits étendus sur des matériels confiés par l'université, leur permettant l'installation de logiciels. Il est rappelé aux usagers qu'un logiciel ne doit pas être installé s'il ne provient pas d'une source fiable. Il convient aussi de respecter les principes suivants :

- installer ou utiliser les logiciels en respectant leurs licences ;
- ne pas installer de logiciels de type « serveur » sans accord de l'université ou de son entité ;
- se conformer aux règles ou dispositions de l'université ou de son entité.

4 Rôle des administrateurs des ressources informatiques

Les administrateurs sont chargés des opérations d'installation, de maintenance, de contrôle des ressources informatiques (réseau, systèmes, applications, données, ...). Les règles s'appliquant à la fonction d'administrateur seront précisées dans une charte des administrateurs.

Ils sont soumis au secret professionnel⁹. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions, même sur ordre de leur hiérarchie, dès lors :

- que ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur ;
- qu'elles ne tombent pas dans le champ de l'article 40 alinéa 2 du code de procédure pénale¹⁰.

Leurs missions les amènent à intervenir sur les ressources informatiques ; y compris les données privées, en cas de risque pour les ressources, d'atteinte à la sécurité ou d'altération au bon fonctionnement technique.

Les administrateurs ont un devoir d'information envers les utilisateurs concernant les mesures, procédures pour le contrôle et la gestion des ressources. En particulier, les utilisateurs doivent être informés lors des opérations de prise de contrôle à distance du poste de travail.

Les utilisateurs doivent se conformer aux prescriptions des administrateurs concernant l'usage des ressources informatiques ou les mesures de sécurité à suivre.

⁹ Ce secret s'applique autant vis-à-vis de personnes extérieures, de membres de l'université ou d'autres administrateurs

¹⁰ Obligation faite à tout fonctionnaire d'informer sans délai le procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions

5 Communications électroniques

L'utilisation d'Internet et des communications électroniques constituent des éléments essentiels comme outil pédagogique, pour la recherche, pour l'optimisation du travail, ou d'une façon générale pour l'accessibilité et la transmission de l'information au sein et en dehors de l'université.

Il est rappelé qu'Internet et toutes les formes de communications électroniques sont soumis à l'ensemble des règles de droit en vigueur.

5.1 Messagerie électronique

5.1.1 Adresses électroniques

L'université s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle ou étudiante nominative¹¹ lui permettant d'émettre et de recevoir des messages électroniques, dans la limite de la disponibilité de cette adresse.

Pour les personnels de l'université, l'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

L'adresse électronique nominative est attribuée à un utilisateur qui la gère sous sa responsabilité.

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 universitaires, désignant une catégorie ou un groupe d'utilisateurs, relève de la responsabilité exclusive de l'université. Ces adresses devront être utilisées dans les conditions prévues.

5.1.2 Contenu des messages électroniques

Pour les personnels de l'université, tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé¹² ou s'il est stocké dans un espace privé de données.

Il est rappelé que les messages électroniques privés sont couverts par le secret des correspondances.

Pour préserver le bon fonctionnement du système de messagerie, des limitations peuvent être mises en place : dans ce cas, les termes en sont précisés dans un guide technique d'utilisation de la messagerie¹³.

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 (Cf. section 7.3).

5.1.3 Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles¹⁴ 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.

¹¹ L'adresse est de la forme prenom.nom@unilim.fr ou prenom.nom@etu.unilim.fr

¹² Pour exemple, les messages comportant les termes ("privé") dans le sujet du message

¹³ Consultez le site web du Service Commun Informatique et le responsable informatique de votre entité

¹⁴ Issus de la loi n° 2004-575 du 21 juin 2004, ces articles fixent certaines obligations pour la conclusion des contrats en ligne

5.1.4 Sécurité

L'université se réserve le droit de filtrer ou d'interdire les messages dont le contenu présente un danger. Lorsqu'un message ou une partie de message sera interdit, le destinataire, ou à défaut l'expéditeur du message, sera averti.

L'université met à la disposition des utilisateurs des outils pour limiter les messages publicitaires envahissants (*spam*), frauduleux, etc.

5.2 Internet

5.2.1 Accès à Internet

L'université met à la disposition de l'utilisateur un accès Internet. L'accès au réseau Internet se fait par le biais du réseau national pour l'éducation et la recherche (RENATER). Son utilisation implique de fait le respect de sa charte déontologique¹⁵.

Internet est un outil de travail ouvert à des usages professionnels, pour répondre aux missions de l'université : il peut constituer le support d'une communication privée telle que définie en section 2.1, dans le respect de la législation en vigueur.

5.2.2 Publications sur les sites internet et intranet de l'université

Tout site de publication Internet doit être autorisé par le Président de l'université.

Les publications doivent comporter les mentions légales obligatoires : dénomination et siège social de l'éditeur, directeur de la publication, responsable de la rédaction, hébergeur, etc., imposées par la loi sur la confiance dans l'économie numérique n°2004-575 du 21 juin 2004. Il est rappelé que le Président de l'université est le directeur de la publication de tout site officiel de l'université (hors sites personnels ou site hébergé pour des personnes morales, entreprises, associations, etc.). Les publications sur les sites Internet officiels de l'université doivent être validées par un responsable de site ou responsable de publication nommément désigné.

Les publications adressées au public français doivent être faites en langue française, comme le précisent la loi du 4 août 1994 (Loi Toubon) et la circulaire du 7 octobre 1999 relative aux sites Internet des services et des établissements publics de l'Etat.

Les publications doivent respecter le référentiel général d'accessibilité pour les administrations (RGAA¹⁶, découlant de l'article 47 de la loi du 11 février, n° 2005-102, pour « l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées »).

Aucune publication de pages d'information à caractère privé (pages privées ...) sur les ressources informatiques de l'université n'est autorisée, sauf disposition particulière prévue par l'université. Dans le cas d'une publication autorisée, l'université, en qualité d'hébergeur, défini dans la loi pour la confiance dans l'économie numérique, n°2004-575 du 21 juin 2004, peut être amenée à supprimer des contenus dont le caractère illicite serait porté à sa connaissance.

5.2.3 Sécurité

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 éventuels dispositifs de sécurité mis en place par l'université. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par l'université.

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais

¹⁵http://www.renater.fr/IMG/pdf/charte_fr.pdf

¹⁶<http://www.references.modernisation.gouv.fr/rgaa-accessibilite/>

d'actions de formations ou de campagnes de sensibilisation.

5.3 Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet (quel que soit le moyen technique utilisé) doit s'effectuer dans le respect des droits de la propriété intellectuelle (Cf. section 7.1).

L'université se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité (virus susceptibles d'altérer le bon fonctionnement, codes malveillants, programmes espions, ...).

6 Traçabilité, surveillance et contrôle des ressources informatiques

6.1 Traces et surveillance

L'université informe l'utilisateur que les ressources informatiques peuvent donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité, dans le respect de la législation applicable.

L'utilisateur est informé que les traces enregistrées ne retiennent pas le contenu même des données échangées, mais seulement les données de connexion¹⁷. La durée de conservation des traces est de 1 an maximum. L'université s'interdit de les exploiter au-delà de 3 mois sauf sur réquisition officielle ou sous une forme rendue anonyme.

Les traces feront l'objet d'une consultation du CIL (voir section 7.2.2), particulièrement pour les traces non prévues par les lois en vigueur.

En dehors des réquisitions réglementaires, seuls les administrateurs peuvent prendre connaissance des traces, et ce à des fins statistiques, de bon fonctionnement ou de sécurité des ressources informatiques.

L'université se dotera d'une « politique de gestion des traces », qui précisera entre autres les différents types de journaux, leurs finalités, les informations enregistrées, les conditions d'accès dont disposent les utilisateurs.

6.2 Contrôle de la sécurité, maintenance

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'université se réserve la possibilité de réaliser des interventions sur les ressources mises à sa disposition ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée ; le cas échéant supprimée.

6.3 Bilan annuel

L'université établira un bilan annuel des incidents de sécurité, des événements ou demandes ayant nécessités des accès particuliers aux traces.

¹⁷ Pour illustration, les traces de la messagerie électronique comportent l'adresse IP des machines sources et destination du message, les adresses méls d'expéditeur et de destinataire apparaissant sur l'enveloppe du message, les identifiants du message, la date et l'heure.

7 Aspects légaux

7.1 Respect de la propriété intellectuelle

L'utilisation des ressources informatiques implique le respect des droits de propriété intellectuelle de l'université, et de ceux de ses personnels¹⁸.

De même, elle implique le respect des droits de ses partenaires et plus généralement, de tous tiers titulaires de tels droits. En conséquence, chaque utilisateur doit :

- utiliser les logiciels en respectant leurs licences ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits, sauf exception pédagogique prévue par la législation.

7.2 Loi « Informatique et Libertés »

7.2.1 Information sur la loi

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 1978 dite « Informatique et Libertés » modifiée par la loi n° 2004-801 du 6 août 2004.

Les données à caractère personnel sont des informations qui permettent, sous quelque forme que ce soit, 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 afférent, 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 les services compétents qui prendront les mesures nécessaires au respect des dispositions légales.

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 ressources informatiques.

Ce droit s'exerce auprès du responsable du traitement des données concernées.

7.2.2 Correspondant « Informatique et Libertés »

Le correspondant à la protection des données à caractère personnel (dit « Correspondant Informatique et Libertés - CIL ») exerce sa fonction dans les conditions prévues par la loi 78-17 du 06 janvier 1978, modifiée, relative à l'informatique, aux fichiers et aux libertés.

L'université est dotée d'un CIL. Il est désigné par le Président de l'université. Il exerce ses missions en toute indépendance, sous le contrôle de la Commission Nationale Informatique et Libertés.

Il est obligatoirement consulté préalablement à la création, modification même mineure, transformation, transfert de données et interconnexion concernant tout traitement informatisé d'informations nominatives mis en œuvre ou hébergé dans l'un quelconque des services de l'université, de ses composantes et de ses laboratoires ou du Service Commun Informatique.

Il veille à la protection des droits des usagers et des personnes concernées par de tels traitements.

Tout utilisateur peut saisir directement le CIL pour accéder à la liste des traitements recensés. Le

¹⁸ Par exemple, documents pédagogiques, données scientifiques, ...

CIL peut également recevoir des réclamations ou requêtes et servir de médiateur avec le responsable du traitement, en veillant au droit d'accès et de rectification.

7.3 Respect des personnes, non-discrimination

L'utilisateur, dans son usage d'Internet et des ressources informatiques, est à la fois protégé par, et tenu de respecter, la loi de 1881 sur la liberté de la presse (qui s'applique par exemple aux sites Internet), imposant un cadre légal à toute publication, ainsi qu'à l'affichage public.

Sont notamment réprimés les actes de diffamation ou d'injure, en particulier en présence d'éléments discriminatoires (racisme, sexisme, homophobie, etc.).

7.4 Respect de la vie privée, droit à l'image

Il est rappelé que les textes, notamment le code pénal et le code civil protègent la vie privée des individus.

En particulier, la publication ou la reproduction d'une photographie sur laquelle une personne est clairement reconnaissable n'est possible qu'avec son consentement préalable, que l'image soit préjudiciable ou non. Font exception à cette règle les photos de foule où la personne n'est pas le sujet central ou bien les photos prises de loin ou de dos.

7.5 Atteintes aux systèmes de traitement automatisé de données

L'utilisateur est informé que l'accès ou le maintien frauduleux dans un système informatique, l'entrave au fonctionnement de celui-ci, la modification ou la suppression frauduleuse des données contenues dans le système, de même que l'introduction frauduleuse de nouvelles données, constitue un délit¹⁹.

8 Limitations des usages

En cas de non-respect des règles définies dans ce règlement ou des modalités définies dans les guides d'utilisation établi par l'université ou l'entité, le Président de l'université ou le responsable d'entité, pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées, limiter les usages par mesure conservatoire, qui devront être proportionnées et à durée limitée.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extraprofessionnelles, est passible de sanctions.

9 Entrée en vigueur du règlement

Le présent règlement est annexé au règlement intérieur de l'université.

Il annule et remplace tous les autres documents, règlements ou chartes relatifs à l'utilisation des ressources ou des moyens informatiques de l'université.

¹⁹ D'après la loi du 5 janvier 1988 (loi dite « Godfrain ») reprises, depuis le premier mars 1994, par les articles 323-1 à 323-7 du Nouveau Code Pénal