Charte d'usage du Système d'Information de l'Université de Montpellier

Charte d'usage du SI UM

Historique des versions du document

Version	Date	Commentaire
1.0	10/06/2024	Version validée

Table des matières

Préambule

Le **cadre de référence de la Sécurité des Systèmes d'Information** (SSI) de l'Université de Montpellier (UM) inclut l'ensemble du corpus documentaire spécifiant et ordonnant les principes et règles à appliquer dans le domaine de la SSI (voir Figure 1).

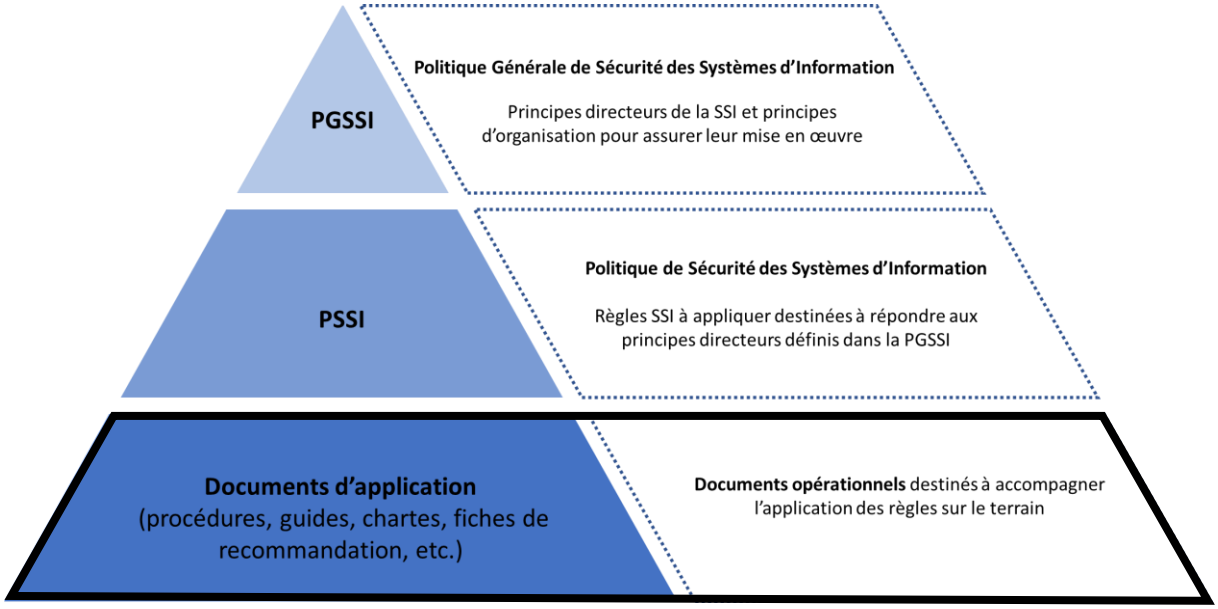

Figure 1 : cadre de référence de la Sécurité des Systèmes d'Information

Au sein de ce cadre de référence SSI, le présent document est un document d'application et constitue la **Charte d'usage du Système d'Information** de l'Université de Montpellier (Charte d'usage du SI UM).

La Charte d'usage du SI UM traite de l'utilisation des **services et solutions numériques** en soutien des activités de l'Université de Montpellier. Dans la suite du document, on confondra Systèmes d'Information (SI) et services et solutions numériques.

Titre 1 – Objet et champ d’application

Article 1 - Objet

La Charte d'usage du SI UM définit les règles d'usage que les utilisateurs du SI UM s’engagent à respecter, afin d’assurer la performance des traitements et la sécurité des données au sein du SI UM.

La Charte d'usage du SI UM ne se substitue pas aux lois et réglementations applicables. Par ailleurs, elle peut être complétée par des guides d'utilisation définissant les pratiques pour des cas d’usage particuliers.

Article 2 - Champ d’application

Toute personne disposant d’un compte d’accès au SI UM est considérée comme un utilisateur du SI UM. La Charte d'usage du SI UM s’applique à l’établissement et à tous les utilisateurs du SI UM, quel que soit leur statut.

Titre 2 : Dispositions générales

Article 3 - Obligations de l’établissement

L'établissement :

- porte à la connaissance de l'utilisateur la présente charte ;
- facilite l’accès des utilisateurs aux ressources du SI UM;
- met en œuvre les mesures nécessaires pour assurer la sécurité du SI UM ;
- met en œuvre les mesures nécessaires pour assurer la protection des données concernant les utilisateurs et des données produites par les utilisateurs.

Article 4 - Obligations de l’utilisateur

L'utilisateur :

- est soumis au respect des obligations résultant de son statut ;
- est responsable, en tout lieu, de l'usage qu’il fait du SI UM, des ressources et des données auxquelles il a accès ;
- doit se conformer aux conditions pour accéder au SI UM et en particulier aux moyens, contrôles et horaires de mise à disposition et / ou de restriction d’accès ;
- doit se conformer aux politiques et procédures en vigueur, dès lors qu’elles sont relatives au SI UM ;
- est responsable de l’intégrité de son espace de travail et du dépôt de ses données sur des espaces adaptés, notamment pour bénéficier des moyens de sauvegarde mis à sa disposition ;
- s’engage à apporter le soin nécessaire au matériel employé pour accéder au SI UM (ex. : ne pas débrancher ou déplacer le matériel sans autorisation préalable, etc.).

Titre 3 : Conditions et règles d’utilisation du SI

Article 5 – Accès au SI

Chaque utilisateur peut se voir attribuer un ou plusieurs moyens d’accès au SI. Ces moyens d’accès sont constitués d’un identifiant unique et nominatif attribué par l’établissement et d’un mot de passe choisi par l’utilisateur, qui peuvent être complétés par des moyens d’authentification complémentaires.

L'utilisateur est informé :

- que ses moyens d’accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive du SI UM ;
- qu’il est responsable de l’utilisation qui est faite de ses moyens d’accès, leur divulgation ou cession volontaire à un tiers engage sa responsabilité pénale, civile et disciplinaire ;
- que ses droits d’accès au SI UM sont définis par l’établissement relativement à son statut et aux fonctions qu’il exerce.

Afin d’assurer la sécurité des accès au SI UM, l’utilisateur est tenu :

- de garder strictement personnel(s) et confidentiel(s) son (ses) moyen(s) d’accès :
  - et ne pas le(s) dévoiler ou le(s) confier à un tiers ;
  - et ne pas les stocker ou les utiliser dans des environnements non institutionnels.
- de respecter les consignes de sécurité et les règles relatives à la gestion des moyens d’accès, en particulier :
  - ne pas utiliser les moyens d’accès d’un autre utilisateur, ni chercher à les connaître ou à les obtenir ;
  - ne pas accéder ou tenter d'accéder à des ressources du SI UM pour lesquelles il n’a pas explicitement reçu d’habilitations ;
  - ne connecter des matériels personnels que sur les SI UM dédiés à cet effet ;
  - ne pas connecter directement au SI UM des matériels ou des périphériques autres que ceux confiés ou autorisés par l’établissement, hors exception ci-avant.

Afin d’assurer la sécurité des accès au SI UM, l’établissement est tenu :

- de veiller à ce que les ressources ne soient accessibles qu’aux personnes habilitées ;
- de supprimer, désactiver ou modifier les droits d’accès dès que la situation le justifie (fin de l'activité, changement de statut, non-respect de la charte, etc.).

Article 6 – Utilisation institutionnelle et privée

L'utilisateur est informé que le SI UM est destiné principalement et prioritairement à des usages institutionnels, administratifs, pédagogiques et en lien avec des activités de recherche ou de documentation (bibliothèque).

L'utilisateur est informé que le SI UM peut néanmoins constituer le support d'une utilisation à titre privé dans les conditions décrites ci-dessous :

- toute information utilisée sur le SI UM est réputée à priori institutionnelle, à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée ;
- l'utilisation du SI UM à titre privé doit respecter la réglementation en vigueur. Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement de l'établissement ;
- il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet ou en mentionnant le caractère privé sur la ressource. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur ;
- l'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'établissement ne pouvant être engagée quant à la conservation de cet espace ;
- l'utilisation résiduelle du SI UM à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. Le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.

Par ailleurs, l'utilisateur :

- ne doit pas stocker sur un dispositif personnel des données institutionnelles ;
- ne doit pas utiliser sa messagerie personnelle pour une communication institutionnelle ;
- ne doit pas utiliser de données institutionnelles en entrée de requêtes vers des systèmes d'Intelligence Artificielle non institutionnels ;
- ne doit pas utiliser de données sensibles en entrée de requêtes vers des systèmes d'Intelligence Artificielle, institutionnels ou non.

Article 7 – Continuité de service

Les données non situées dans un espace identifié comme privé sont considérées comme appartenant à l'établissement qui pourra en disposer.

Afin d'assurer la continuité de service :

- l'utilisateur doit privilégier le dépôt de ses fichiers de travail sur des zones partagées pour le travail collaboratif ;
- l'utilisateur doit prévoir une réponse automatique d'absence sur sa messagerie identifiant un correspondant alternatif et en cas de manquement, l'établissement pourra procéder à la mise en place du dispositif.

En cas de départ ou d’absence prolongée, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition et, autant que possible, rend disponibles les éléments professionnels en sa possession.

Article 8 – Utilisation des ressources techniques du SI

L’utilisateur est tenu :

- de ne pas tenter de modifier la configuration des ressources ou de contourner les dispositifs de sécurité du SI UM ;
- de ne pas installer au sein du SI UM, pour son propre usage, une ressource non autorisée par l’établissement (ex. : point d’accès sans fil, équipements type IoT, etc.) ;
- de ne jamais quitter un poste de travail sans verrouiller sa session de travail ;
- de ne jamais quitter un poste de travail en libre-service sans se déconnecter ;
- de prendre les précautions adaptées (utilisation d’un câble antivol, d’un filtre de confidentialité, etc.) et d’adopter une posture vigilante en situation de mobilité, en fonction de différentes situations rencontrées (ex. : lieux publics) ;
- de prendre les précautions adaptées (séparation des activités privées et professionnelles, non-utilisation de moyens d’impression ou de stockage externe privé, etc.) en situation de télétravail ;
- de réaliser aux moments qui pénalisent le moins les utilisateurs, les tâches risquant d’accaparer fortement les ressources (impression de gros documents, calculs importants, utilisation intensive du réseau, etc.).

Article 9 – Utilisation des logiciels, données et applications

L’utilisateur est tenu :

- de ne pas consulter, détenir, diffuser et importer des données à caractère pédopornographiques, d’incitation à la discrimination, à la haine ou à la violence ou présentant un caractère raciste ou discriminatoire ;
- de ne pas télécharger, reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies, sons, musiques, vidéos ou autres créations protégées par le droit de propriété intellectuelle, en particulier le droit d’auteur ou un droit privatif, sans avoir obtenu préalablement l’autorisation des titulaires de ces droits ;
- de ne pas consulter, supprimer ou altérer des informations ou données détenues par d'autres utilisateurs sans leur autorisation, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type messagerie électronique dont l'utilisateur n'est destinataire ni directement, ni en copie ;
- de ne pas installer, télécharger ou utiliser volontairement sur le SI UM :
    - des logiciels non autorisés par l’établissement ou non conformes aux missions de l’établissement (ex. : logiciels à caractère ludique, etc.) ;
    - des logiciels ou progiciels dont les droits de licence n’ont pas été acquis, ou ne provenant pas de sites de confiance ;

- des codes ou logiciels malveillants.

- de ne pas utiliser de moyens externes non autorisés par l'établissement pour stocker ou transmettre de la donnée (ex. : stockage ou échange de données via des espaces cloud, redirections vers des mails externes – hors partenaires, etc.) ;
- de ne pas réaliser des copies de logiciels soumis à licence (exceptées les copies de sauvegarde) ou de mettre à disposition ce logiciel à une tierce personne par l'intermédiaire du réseau ;
- de ne pas contourner les restrictions d'utilisation d'un logiciel autorisé ;
- d'informer l'établissement préalablement à tous traitements relatifs à des données à caractère personnel, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers ou de données préexistants ;
- de signaler au responsable de l'application source tout constat concernant une donnée de gestion (ex : numéros de téléphone, etc.) qui nécessiterait une mise à jour ;
- de respecter la politique de sécurité de l'application, ainsi que les règles et procédures en vigueur, lors de toute manipulation de données extraites du SI.

Lors d'un changement de poste ou d'habilitations d'un utilisateur, le responsable de l'utilisateur concerné a pour obligation d'informer le service compétent conformément à la procédure en vigueur.

Article 10 – Utilisation d'internet

10-1 – Accès à Internet

Il est rappelé à l'utilisateur que :

- l'usage d'Internet est soumis à la législation en vigueur (cf. Annexe 3 – Lois et réglementations) ;
- pour l'accès à Internet depuis le SI, les chartes des différents fournisseurs d'accès au réseau Internet s'appliquent (ex. : Charte RENATER) ;
- si une utilisation résiduelle privée, telle que définie en article 6 peut être tolérée, les accès à Internet à partir du SI UM sont présumés avoir un caractère institutionnel ;
- l'accès à Internet à partir du SI UM de l'établissement n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'établissement et doit respecter la politique en vigueur ;
- toute utilisation d'Internet contraire aux dispositions définies engagera la responsabilité personnelle de l'utilisateur.

L'établissement se réserve le droit de filtrer ou d'interdire l'accès à Internet, de procéder au contrôle *a priori* ou *a posteriori* des connexions, des durées d'accès et des volumétries d'utilisation correspondantes en application du principe de précaution, en cas d'incident, d'abus ou de réquisition judiciaire.

10-2 – Publication sur les sites et réseaux sociaux de l'établissement

Toute publication de pages d'information sur les sites internet ou intranet de l'établissement doit être validée selon la procédure d'hébergement en vigueur.

L'utilisateur veillera donc à ne pas communiquer sur les sites web, blogs ou réseaux sociaux de l'établissement des informations professionnelles non vérifiées ou pouvant nuire à l'établissement ou compromettre son image, ainsi que des informations à caractère confidentiel. Par ailleurs, il ne s'exprimera au nom de l'établissement qu'avec son autorisation préalable.

Aucune publication de pages d'information à caractère privé sur le SI UM de l'établissement n'est autorisée, sauf disposition particulière.

10- 3 – Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des droits de propriété intellectuelle (cf. Annexe 3 – Lois et réglementations).

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

Article 11 – Communication électronique

11-1 – Adresses électroniques

L'établissement s'engage à mettre à disposition de l'utilisateur une boite aux lettres institutionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative est ensuite de 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 institutionnel de la messagerie.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'établissement.

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 ; ces listes ne peuvent être utilisées sans autorisation explicite.

11-2 – Contenu des messages électroniques

Tout message électronique est réputé à priori institutionnel, sauf s'il comporte une mention particulière et explicite indiquant son caractère privé ou s'il est stocké dans un espace privé de données.

La messagerie électronique ne doit pas être utilisée pour le transfert de fichiers volumineux, pour lesquels il est préconisé d'utiliser des moyens adaptés.

Pour préserver le bon fonctionnement des services, l'établissement se réserve le droit de mettre en place des limitations.

Les messages comportant des contenus à caractère illicites sont interdits 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 (ex. : atteinte à la tranquillité par les menaces, atteinte à l'honneur et à la considération par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques, etc.).

11-3 – Émission et réception des messages

L'utilisateur est tenu :

- de s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages ;
- de veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés ;
- d'utiliser des listes de diffusion pour répondre aux besoins de diffusion de messages en masse ;
- de signaler les mails suspects à l'adresse abuse@umontpellier.fr.

11-4 – Statut et valeur juridique des messages

Les messages électroniques échangés avec les tiers peuvent, sur le plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1125 à 1127-4 du code civil relatifs aux contrats conclus par voie électronique.

L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que les courriers traditionnels.

11-5 – Stockage et archivage des messages

Chaque utilisateur doit organiser et mettre en œuvre, dans l'environnement qui lui est dédié par l'établissement, les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

Article 12 – Devoir de signalement

L'utilisateur est tenu :

- d'avertir son responsable ou la DSIN dans les meilleurs délais de tout dysfonctionnement constaté ou toute anomalie découverte relative au SI UM (ex. : vol, intrusion dans le SI) ;
- de signaler à la personne responsable toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

Article 13 – Exploitation et contrôle du SI

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'établissement se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur le SI UM ;
- qu'une opération de maintenance qui nécessite une prise en main à distance d'une session utilisateur doit obligatoirement être précédée d'un accord de l'utilisateur ;
- que toute information bloquante pour le système ou générant une difficulté technique sera isolée et, le cas échéant, supprimée ;

- que les journaux d'événement produits par le SI UM peuvent être exploités 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.

Les personnels chargés des opérations de contrôle du SI sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou identifiées comme telles.

En revanche, ils doivent communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité, ou en cas de réquisition judiciaire.

Article 14 – Traçabilité légale du SI

L'établissement est dans l'obligation légale de mettre en place un système de journalisation de certains usages du SI, tels que les accès Internet ou la messagerie.

L'établissement procédera à l'inscription au registre des traitements de données à caractère personnel auprès de Délégué à la Protection des Données, dans le cas où les traces comporteraient des données à caractère personnel, qui mentionnera notamment la durée de conservation des traces et durées de connexions et les conditions du droit d'accès dont disposent les utilisateurs.

Titre 4 – Dispositions finales

Article 15 – Entrée en vigueur

La présente Charte d'usage du SI UM a été soumise pour avis au Comité Social d'Administration (CSA) du 3 juin 2024 et est applicable immédiatement. Elle annule et remplace toutes les chartes précédentes relatives à l'usage du SI UM.

Pour toute demande (commentaire, question, etc.) concernant la présente Charte d'usage du SI UM, veuillez contacter la Direction des Affaires Générales et Institutionnelles de l'Université de Montpellier.

Article 16 – Sanctions applicables

Les utilisateurs du SI UM sont tenus de respecter l'ensemble des règles édictées dans la Charte d'usage du SI UM ainsi que dans les guides d'utilisation établis par l'établissement. Tout manquement est susceptible d'entraîner des sanctions disciplinaires, dont :

- la suspension, la suppression ou la limitation des accès et / ou des droits d'utilisation du SI
- les poursuites disciplinaires, civiles et pénales prévues par les textes législatifs et réglementaires en vigueur.

Par ailleurs, la personne juridiquement responsable pourra, sans préjuger des poursuites ou procédures pouvant être engagées à l'encontre des utilisateurs, limiter les usages par mesure conservatoire.

Annexe 1 – Acronymes

CNIL	Commission Nationale de l'Informatique et des Libertés
DPO	Délégué à la Protection des Données (DPO pour *Data Privacy Officer*)
IA	Intelligence Artificielle
IOT	Objet connecté (IoT : *Internet of Things* / Internet des Objets)
PPST	Protection du Patrimoine Scientifique et Technique
PSSI	Politique de la Sécurité des Systèmes d'Information
RGPD	Règlement Général sur la Protection des Données
SI	Système d'Information
SSI	Sécurité des Systèmes d'Information
UEI	Unités de formation et de recherche, Ecoles et Instituts
UM	Université de Montpellier

Annexe 2 – Définitions

Code ou logiciel malveillant	Code ou logiciel développé dans le but de nuire à un SI. Les virus, vers, chevaux de Troie ou bombes logiques constituent des exemples de codes ou de logiciels malveillants.
Donnée à caractère personnel	Des données sont considérées comme à caractère personnel dès lors qu'elles permettent d'identifier directement ou indirectement des personnes physiques. Ex. : nom, n° d'immatriculation, n° de téléphone, photographie, éléments biométriques tels que l'empreinte digitale, ADN, numéro d'identification national étudiant (INE), identifiant, adresse IP, ensemble d'informations permettant de discriminer une personne au sein d'une population (certains fichiers statistiques) tels que, par exemple, le lieu de résidence, profession, sexe, âge, etc.
Etablissement	Toute unités de formation et de recherche, écoles et instituts (UEI) et structures de recherche de l'Université de Montpellier.
Institutionnel	Propre aux activités de l'établissement
Messagerie	La messagerie électronique comprend les systèmes de courrier électronique, de messagerie instantanée et messagerie texte (SMS)
Personne juridiquement responsable	Toute personne ayant la capacité de représenter l'établissement (directeur, chef d'établissement, etc.).
Responsable de l'utilisateur	Le responsable de l'utilisateur est : - Pour les agents titulaires ou non titulaires concourant à l'exécution des missions du service public de l'éducation et les stagiaires : le responsable hiérarchique ; - Pour les enseignants, chercheurs et enseignants chercheurs : le directeur de l'unité de formation, école ou institut ou de la structure de recherche ; - Pour les étudiants : l'enseignant ; - Pour les prestataires : le responsable du contrat de prestation.
Système d'information	Ensemble des ressources techniques, applicatives, organisationnelles, humaines et documentaires permettant de collecter, stocker, traiter, rechercher et/ou transmettre des données, en particulier : - Tout matériel informatique fixe : postes (dont les postes en libre-service), serveurs, téléphones, périphériques (clavier, écran, imprimante, etc.), prises, câbles, etc. - Tout matériel informatique mobile : ordinateur, téléphone, etc. - Tout logiciel ou service réseau ou informatique : accès réseau, accès internet, messagerie électronique, bureautique, service numérique, applicatif, etc. - Tout support de données : électronique, papier, etc.
Système d'information mobile	Ensemble des ressources mobiles du SI UM ou des ressources permettant l'utilisation du SI UM avec des ressources mobiles Ex. : clés USB, assistants personnels, ordinateurs portables, téléphones portables de type Smartphones, accès wifi, etc.

Utilisateur

Toute personne physique ou morale utilisant les ressources du SI UM, quel que soit son statut, en particulier :

- Tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'éducation ;
- Tout enseignant, enseignant-chercheur, chercheur ou doctorant utilisant les ressources de l'université, y compris les locaux ;
- Tout personnel hébergé utilisant les ressources de l'université, y compris les locaux ;
- Tout étudiant inscrit ou en cours d'inscription pour l'année en cours, ou ayant été inscrit à l'université ;
- Tout prestataire ayant contracté avec l'établissement ;
- Tout stagiaire utilisant les ressources de l'université, y compris les locaux.

Secret professionnel

Un agent public ne doit pas divulguer les informations personnelles dont il a connaissance.

Cette obligation s'applique aux données à caractère personnel, dont téléphone, mail, adresse postale, mais aussi informations relatives à la santé, au comportement, à la situation familiale d'une personne, etc.

Annexe 3 – Lois et réglementations

Nota : les éléments proposés ci-après ont une valeur informative et ne visent pas l'exhaustivité.

Propriété intellectuelle

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

Les droits de propriété intellectuelle sont régis par le Code de la propriété intellectuelle et par la loi n°92-597 du 1er juillet 1992.

Protection des données à caractère personnel

L'utilisateur et l'établissement sont tenus de respecter les dispositions légales en matière de protection des données à caractère personnel, conformément au règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (Règlement Général sur la Protection des Données - RGPD).

Le RGPD établit des principes fondamentaux pour le traitement des données à caractère personnel, exigeant la transparence, la légitimité, la limitation de la finalité, la minimisation des données, l'exactitude, la limitation de la conservation et l'intégrité et la confidentialité des données.

Conformément au RGPD, les responsables de traitement sont tenus de documenter, en interne, les violations de données personnelles et de notifier les violations présentant un risque pour les droits et libertés des personnes à la CNIL et, dans certains cas, lorsque le risque est élevé, aux personnes concernées.

Par ailleurs, conformément aux dispositions du RGPD, chaque utilisateur dispose

- des droits d'accès, de rectification et d'effacement de ses données personnelles ;
- du droit de limitation du traitement de ses données personnelles ;
- du droit de retirer son consentement pour l'avenir.

Ces droits s'exercent auprès du responsable de l'utilisateur ou auprès du Délégué à la Protection des Données (DPO) de l'Université de Montpellier.

Pour toute question relative au RGPD et à son application au sein de l'université de Montpellier, s'adresser à dpo@umontpellier.fr

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.

Diffusion de l'information

L'utilisation des moyens informatiques mis à disposition par l'établissement doit respecter la réglementation en vigueur. En particulier, la diffusion de messages diffamatoires ou injurieux, les provocations et apologies (crime, racisme, négationnisme, crimes de guerre, ...), l'accès,

la détention, la diffusion d'images à caractère pédophile, la publication d'informations confidentielles sans autorisation préalable ou en violation du droit de la propriété intellectuelle sont strictement interdits.

Protection du Potentiel Scientifique et Technique (PPST)

Le dispositif de protection du potentiel scientifique et technique de la nation (PPST) a pour but de protéger, au sein des établissements publics et privés localisés sur le territoire national, l'accès aux savoirs et savoir-faire stratégiques ainsi que les technologies sensibles. Il permet de se prémunir plus efficacement contre les tentatives de captation ou de destruction d'informations.

Le dispositif PPST offre une protection juridique et administrative fondée sur le contrôle des accès, physiques comme virtuels, aux informations stratégiques ou sensibles détenues au sein de zones protégées spécifiques, appelées zones à régime restrictif (ZRR).

Charte RENATER

Le Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche (RENATER) fournit une connectivité nationale et internationale aux établissements de cette communauté à laquelle appartient l'établissement. Les règles d'usage de RENATER (réseau réservé à une utilisation professionnelle) sont définies par une charte déontologique qui s'impose à tous les utilisateurs.

L'usage commercial à titre privé est proscrit.

Autres lois et règlementations applicables

L'utilisateur et l'établissement sont tenus de respecter les dispositions légales et réglementaires suivantes :

- l'article 29 de la loi du 29 juillet 1881 relatif à la diffamation ;
- la loi du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunication ;
- le décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques ;
- la loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels ;
- la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;
- la loi n°2004-575 du 21 juin 2004 pour la confiance en l'économie numérique (dite « loi LCEN ») :
- les articles L.323-1 et suivants du code pénal relatifs aux atteintes aux systèmes de traitement automatisé de données ;
- la loi n°88-19 du 5 janvier 1988, modifiée (dite « loi Godfrain ») relative à la fraude informatique ;
- l'article 9 du code civil relatif au droit à la vie privée ;
- les articles R226-1 et suivants, R623-4 et R625-9 du code pénal relatifs aux atteintes à la vie privée ;

- l’article 227-23 du code pénal relatif à la sanction pénale de la consultation habituelle (sur Internet), de l'enregistrement, de la diffusion et de la détention d'images pédopornographiques ;
- les articles R625-7 et suivants du code pénal relatifs à la sanction pénale de l’incitation à la discrimination, à la haine ou à la violence ;
- les articles R624-3 et suivants du code pénal relatifs à sanction pénale de la diffusion de données présentant un caractère raciste ou discriminatoire ;
- l’article R621-1 du code pénal relatif à la sanction pénale de la diffamation ;
- les articles 1369-1 à 1369-11 du code pénal relatifs aux contrats sous forme électronique.