

CHARTRE GENERALE A L'USAGE DES RESSOURCES NUMERIQUES

Université Clermont Auvergne

Table des matières

1.	Contexte et définitions	2
1.1	Introduction.....	2
1.2	Définitions	2
1.3	Risques et opportunités	4
1.4	Caractère opposable de la charte générale	4
2.	Usage des Ressources numériques	5
2.1	Définitions	5
2.2	Autorisation et protection de l'Accès aux Ressources numériques.....	6
2.3	Modification et suppression des Autorisations d'Accès	8
2.4	Droits relatifs aux données numériques produites dans l'exercice d'une mission professionnelle par un agent	9
2.5	Accès illégitime aux données numériques professionnelles et personnelles.....	10
2.6	Le transfert de données par un Usager.....	10
2.7	Continuité de service : gestion des absences et des départs.....	11
3.	Devoir d'information	12
3.1	Devoir d'information auprès de l'Etablissement par les Usagers	12
3.2	Devoir d'information auprès des Usagers par l'Etablissement.....	12
4.	Surveillance du réseau et des Ressources informatiques	13
5.	Droit à la déconnexion	14
6.	Chartes spécifiques	14
7.	Exemples de pratiques contrevenant à la charte générale.....	15
8.	Les sanctions et les textes de référence.....	17
8.1	Sanctions	17
8.2	Principaux textes législatifs et sanctions se rapportant à la sécurité des systèmes d'information et à la protection des personnes.....	17
9.	Diffusion et révision de la charte générale	18

1. Contexte et définitions

1.1 Introduction

L'usage de ressources numériques est devenu systématique, commun et indispensable au déroulement des missions des universités et de leurs usagers. Les ressources numériques sont également devenues l'objet de nombreuses convoitises et de détournement à des buts malveillants, constituant autant d'actes illégaux ou indésirables pour l'établissement.

Le présent document nommé « Charte générale pour l'usage des ressources numériques » a pour objet de décrire les conditions dans lesquelles les ressources numériques de l'Université Clermont Auvergne peuvent être utilisées par l'ensemble des usagers, et de préciser la responsabilité des usagers et de l'établissement en accord avec la législation et la réglementation. Il définit les règles de bonne utilisation et participe à la prise de conscience des devoirs, des responsabilités et des sanctions. Il est en ce sens un outil de protection des usagers et de l'établissement.

Cette charte générale s'adresse à l'ensemble des usagers de l'Université Clermont Auvergne, elle est opposable à tous. Le non-respect de cette charte engage la responsabilité personnelle de l'utilisateur. Elle est annexée au règlement intérieur de l'établissement.

La présente charte générale a été présentée devant le comité technique puis au conseil d'administration qui en a validé les termes et s'est prononcé favorablement pour son application à l'ensemble des Usagers. Ainsi, son acceptation par tout Usager devient une condition préalable à l'Accès aux Ressources numériques de l'Etablissement.

1.2 Définitions

Dans la présente charte, les termes principaux, identifiés par une majuscule, répondent aux définitions et commentaires suivants :

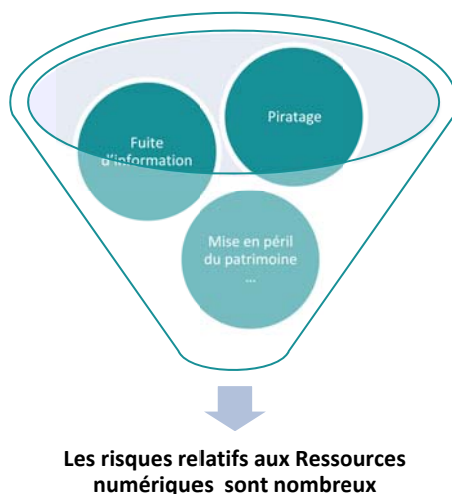
Terme utilisé	Définition	Commentaires
Etablissement	l'Université Clermont Auvergne	Prise en tant que personne morale disposant d'une capacité juridique
Administrateur	Agent ou prestataire chargé par la direction des systèmes d'information de l'Université Clermont Auvergne d'administrer et contrôler l'utilisation d'un système d'information ou de Ressources numériques de l'Université	
Usager	Apprenant (étudiant, stagiaire, ...) ou autre personne physique (agent de l'UCA, intervenant extérieur) qui agissant pour son propre compte ou celui de son employeur utilise les ressources numériques de l'établissement dans le cadre d'une accréditation qu'il a reçu de l'Etablissement	Il s'agit des personnels permanents ou non et des intervenants hébergés, des étudiants, stagiaires et auditeurs, des partenaires, des fournisseurs et des invités qui interviennent temporairement dans un cadre contractuel défini.
Ressource(s) numérique(s)	Données numériques et tous moyens, composants, ou services numériques contribuant à accéder, collecter, stocker, transformer, diffuser ces données numériques	Qu'ils soient matériels ou logiciels, hébergés sur des serveurs internes ou externes exploités sous la responsabilité de l'Etablissement
Mission	Périmètre d'intervention légitime d'un Usager vis-à-vis de l'Etablissement	Il s'agit d'une mission professionnelle, d'une prestation, d'une inscription à un cursus d'apprentissage, de la participation à une conférence, de la fourniture de produits ou services, dont la finalité est établie, en fonction des usagers.
Accès ou accéder	Fait d'utiliser une Ressource numérique	L'Accès est entendu comme utilisation légitime, ayant nécessairement fait l'objet d'une Autorisation
Autorisation ou autoriser	Décision prise par l'Etablissement et conférant un caractère légitime à l'Accès à une Ressource numérique	-
Tiers	Désigne une personne physique ou morale différente de l'Etablissement	Le Tiers est qualifié de « conventionné » lorsqu'il a conclu avec l'Etablissement un accord autorisant ses Usagers à utiliser les Ressources numériques du Tiers
Charte(s) spécifique(s)	Chartes détaillées et dédiées à l'utilisation de ressources numériques à diffusion restreinte.	Ces chartes ne s'imposent qu'au cas par cas à des sous-ensembles restreints d'Usagers

1.3 Risques et opportunités

Les principes exprimés dans ce document sont applicables de façon générale et adaptés à la majorité des environnements.

Chaque Usager est invité à s'appropriier le présent document, tant dans l'intérêt de sa mission auprès de l'Etablissement que dans son intérêt propre.

Afin d'utiliser les Ressources numériques de manière optimale, et de se prémunir contre les risques principaux.



1.4 Caractère opposable de la charte générale

L'utilisation des Ressources numériques mises à disposition par l'Etablissement implique un respect strict de la présente charte générale par chaque Usager. La charte générale présente un caractère opposable.

2. Usage des Ressources numériques

2.1 Définitions

Pour les besoins de l'accomplissement de leurs Missions, l'Université met à la disposition de ses Usagers des Ressources numériques présentées dans le tableau ci-dessous :

Ressources numériques

- ➔ **Infrastructure réseaux** : à portée locale, nationale (Renater) et publique, que ces infrastructures soient filaires ou non filaires
- ➔ **Données collectées et produites** : que ce soit dans le domaine administratif, pédagogique, documentaire ou de la recherche
- ➔ **Matériels informatiques** : ordinateurs fixes et portables, serveurs, tablettes, smartphones et sous-jacents : serveurs, switches, firewall
- ➔ **Applications** : portails internet, extranet, intranet, logiciels et progiciels de gestion, logiciels et progiciels spécialisés, logiciels et progiciels bureautiques et utilitaires, messagerie
- ➔ **Support d'identification et d'authentification** : badges étudiants et personnels RFID, cartes magnétiques, certificats de signature numérique
- ➔ **Espaces de stockage** : internes, externes et mobiles
- ➔ **Matériels techniques accédant aux ressources** : téléphonie fixe et mobile, moyens de reprographie, périphériques connectés, fax
- ➔ **Tout produit ou service numérique** : dès lors que pour être utilisé il nécessite le recours à l'un ou l'autre des produits ou services mentionnés ci-dessus
- ➔



A noter : Tout accès à des moyens ou services numériques tiers depuis un matériel ou des réseaux de l'Etablissement, implique de fait l'accès à des ressources numériques de l'établissement.

2.2 Autorisation et protection de l'Accès aux Ressources numériques

L'Accès à chacune des ressources numériques est soumis à Autorisation. Une Autorisation s'obtient soit automatiquement en fonction de profils d'Usagers, soit sur demande par voie hiérarchique, ou encore lorsque ne sont pas établis de liens hiérarchiques, par une demande auprès du représentant administratif d'une entité dans laquelle s'opère la Mission.

Cette Autorisation est confiée à titre personnel par l'Administrateur à chaque Usager et pour une durée déterminée correspondant le plus souvent à la durée de sa Mission.

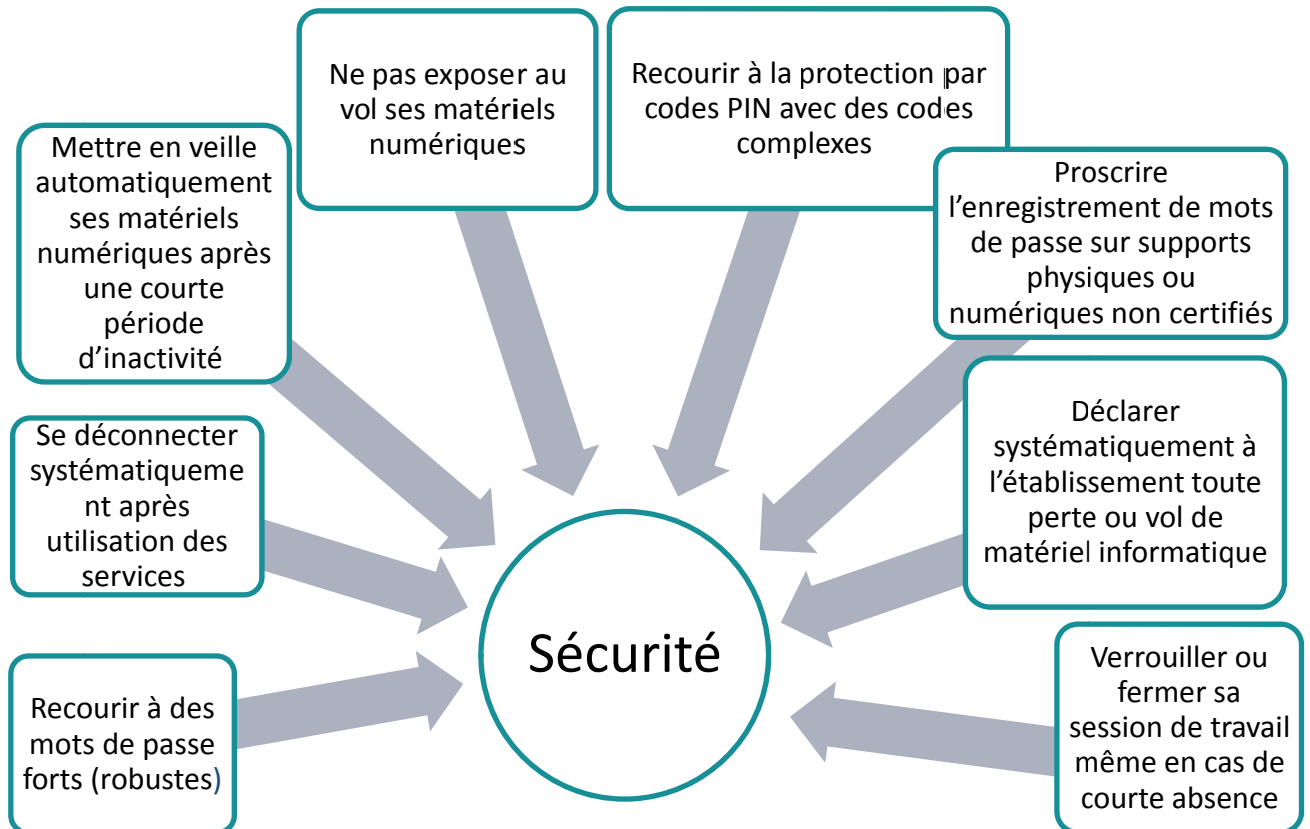
L'Autorisation s'accompagne de la délivrance à l'Usager par l'Administrateur d'un identifiant et d'un mot de passe confidentiel et strictement personnel. Ces moyens d'authentification sur le réseau informatique et plus généralement vis-à-vis des Ressources numériques de l'Etablissement ne doivent être en aucun cas ni communiqués ni cédés à un Tiers.

Il appartient à chaque Usager de prendre les précautions nécessaires pour protéger ses identifiants, afin que ceux-ci ne soient pas divulgués à des Tiers. Le compte informatique en particulier est strictement personnel et inaccessible. Il en est de même pour tout moyen d'identification/authentification physique ou numérique (par exemple certificat de signature électronique).



A savoir : Chaque Usager est responsable de l'utilisation qu'il fait des Ressources numériques via les Autorisations d'accès qui lui ont été confiées.

Pour se protéger, l'Établissement recommande à ses Usagers les mesures suivantes :



Liste non exhaustive donnée à titre indicatif

A ces fins, l'utilisateur qui en fait la demande (contacts disponibles dans les « mentions légales » du site web de l'université), peut prendre connaissance des documents de référence, internes ou externes. Ils déclinent les bonnes pratiques en matière de protection d'Accès en cas de menace potentielle ou avérée du patrimoine informationnel de l'Établissement.

L'Usager ne peut s'opposer au droit de l'Établissement d'accéder à toutes Ressources numériques, y compris les ressources matérielles qui lui auront été prêtées. Les interventions menées par les équipes techniques, sous la direction et le contrôle de l'Administrateur se déroulent de deux manières :

- **Intervention à distance** : l'équipe technique prend le contrôle du matériel avec l'accord préalable de l'Usager.

- **Intervention physique** : lorsque nécessaire, l'équipe technique fixe un rendez-vous à l'Usager qui s'engage à rendre disponible le matériel requis. Il peut obtenir un matériel de prêt sous réserve de disponibilité.



A savoir : un administrateur de systèmes ne demandera jamais à un usager de lui communiquer son mot de passe (ni par courriel, ni de visu). Il pourra exceptionnellement l'inviter à se connecter à un système auquel il doit accéder au nom de l'Usager pour les besoins de sa Mission. Les mots de passe sont enregistrés dans les serveurs universitaires sous forme sécurisée, si bien qu'un administrateur lui-même ne peut les relire.

En cas d'absence de l'Usager (arrêt maladie, déplacement, congé, etc.) ou d'impossibilité pour l'Administrateur d'entrer en contact avec lui et s'il est fait obligation à l'Administrateur d'accéder aux données de l'Usager pour des motifs de sécurité ou d'exploitation, l'Etablissement se réserve la faculté de prendre toutes mesures nécessaires pour accéder aux données. Il est rappelé à cet égard que lorsqu'un accès aux données professionnelles est requis et en cas d'absence de l'agent dans une situation d'urgence risquant de conduire à un blocage ou un dysfonctionnement, la loyauté des relations entre l'Etablissement et l'agent autorise ce premier à accéder aux données de l'agent. Toute intervention dans ce sens se fera toutefois dans le respect de la vie privée conformément aux mesures prises préventivement par l'agent lui-même (cf paragraphe 2.4 de la présente charte, section « vie privée » à ce sujet).

2.3 Modification et suppression des Autorisations d'Accès

Toute Autorisation relative à l'usage des Ressources numériques prend fin naturellement lors de la cessation de la Mission auprès de l'Etablissement (fin de contrat ou d'année universitaire notamment). L'Autorisation peut être modifiée en fonction des évolutions de la Mission de l'Usager et/ou de la politique de l'établissement dans le sens d'une extension ou d'une restriction des droits d'Accès.

Un manquement au respect de la présente charte générale constitue un motif valable de modification, de suspension, voire de suppression d'une Autorisation.

A l'issue de la Mission de l'Usager, l'Etablissement est chargé de restituer les éventuelles données qui appartiendraient en propre à l'Usager et qui seraient conservées dans les Ressources numériques. L'Usager devra manifester son intention de les récupérer ou de les voir supprimer.

Les messages électroniques qui seraient adressés à l'Usager, après expiration de ses droits d'Accès aux Ressources numériques et suppression de ses données seront rejetés des systèmes de messagerie de l'Etablissement.

2.4 Droits relatifs aux données numériques produites dans l'exercice d'une mission professionnelle par un agent

Lorsqu'elles sont produites dans l'exercice d'une mission professionnelle, les données numériques sont de façon générale réputées être à caractère professionnel et appartenir dès lors à l'employeur. Certaines données dérogent néanmoins à ce cadre, lorsqu'elles relèvent de :

- la création d'œuvres de l'esprit pour laquelle l'agent n'a pas été explicitement missionné
- la vie privée, au titre du droit à la vie privée résiduelle qui peut s'exercer sur le lieu du travail dans les limites légales.

Œuvres de l'esprit

Le code de la propriété intellectuelle reconnaît aux auteurs de création d'œuvres de l'esprit un droit de titularité (également nommé droit d'auteur) qui s'exerce sous forme d'un droit moral inaliénable, et de droits patrimoniaux transférables et cessibles. L'employeur conserve le droit d'exploitation lorsqu'une œuvre de l'esprit a été créée dans le cadre de la mission professionnelle d'un agent et que l'agent a été missionné pour la réaliser. Une exception s'appliquant particulièrement au contexte universitaire concerne notamment les productions scientifiques et d'enseignement pour lesquels l'employeur peut ne pas bénéficier systématiquement de droit d'exploitation tacite dans la mesure où il n'oriente pas systématiquement la création des œuvres de l'esprit.

Vie privée

De même, l'intimité de la vie privée et le secret des correspondances électroniques privées sont garantis à l'Usager sauf dans les cas où la loi autorise leur limitation.

S'agissant des agents de l'établissement, un usage à titre personnel des ressources numériques professionnelles est toléré tant qu'il reste modéré et n'interfère pas avec leur mission professionnelle, et ce conformément au principe connu sous la dénomination de « vie privée résiduelle ». Cette tolérance d'usage porte autant sur les fichiers de données que sur les correspondances électroniques. Lorsqu'il s'agit de données personnelles ou de correspondances personnelles sous forme numérique, celles-ci doivent être identifiées explicitement comme telles sous la désignation de « privé et confidentiel » ; toute autre dénomination sera considérée comme non-opérante par l'Etablissement, conférant alors aux données un caractère professionnel. Pour autant, cette pratique n'exempte pas leurs détenteurs de se soumettre à la législation, notamment relative aux droits d'auteur des tiers et aux contenus illicites. L'ensemble des données privées et non-professionnelles restent accessibles dans le cadre d'une réquisition judiciaire.



A savoir : détenir illégalement des contenus protégés par les droits d'auteur (exemples : films, musiques, logiciels) sur un support professionnel engage à la fois la responsabilité de l'employeur pour contrefaçon et celle de la personne qui les a introduits. Ainsi accéder ou maintenir de tels contenus sur des espaces de stockage fournis par l'Etablissement constitue une faute.

Toutes autres données numériques manipulées dans le cadre d'une mission professionnelle sont réputées à caractère professionnel.

2.5 Accès illégitime aux données numériques professionnelles et personnelles

L'Etablissement déploie des moyens conséquents pour assurer la sécurité de ses Ressources numériques. Pour autant le niveau de sécurité est dépendant de nombreux facteurs. Certains dépendent directement de Tiers et dès lors ils ne peuvent être totalement maîtrisés par l'Etablissement, indépendamment des moyens déployés. Par ailleurs la volumétrie importante des systèmes sous-jacents est telle qu'elle ne permet pas à l'Etablissement de se prémunir totalement de tous types d'attaques malveillantes.

L'Accès aux données de toutes natures stockées sur les serveurs de l'Etablissement ne saurait constituer un Accès illégitime lorsqu'il est opéré par un administrateur technique dans le cadre strict de sa mission, ou par un prestataire placé sous sa responsabilité. La charte des administrateurs techniques protège les Usagers en ce sens, et définit les finalités pour lesquelles un administrateur technique intervient sur les données des Utilisateurs, et notamment : besoin de gestion (déplacement de fichier, sauvegarde, renouvellement de matériel), inspection extraordinaire sur incident ou alerte de sécurité informatique, réponse à une requête judiciaire. L'Etablissement est garant vis-à-vis des Usagers du strict respect de cette charte par les administrateurs techniques.

2.6 Le transfert de données par un Usager

Le transfert de données numériques est qualifié d'usage de Ressources numériques en ce qu'il utilise d'autres ressources numériques de l'Etablissement telles que le stockage ou les réseaux. Le transfert de données peut constituer une source de fuite ou de vol de données. Le transfert de données appartenant à l'Etablissement et opéré par un Usager lorsqu'il est agent, vers des tiers ou à destination d'un espace de stockage externe à l'Etablissement, ne peut s'effectuer que dans les termes d'une convention et sous le contrôle de l'Administrateur. Il doit être réalisé dans un cadre strict d'autorisation donnée par le représentant légal de l'Etablissement, que ce transfert relève directement ou non de la mission de l'agent.

En ce qui concerne la diffusion d'informations nominatives, elle n'est possible que dans le respect des prescriptions figurant à l'article 15 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Aucun Usager n'est a priori autorisé à procéder à un quelconque traitement (au sens de la loi « Informatique et Libertés ») de données à caractère directement ou indirectement personnel à l'aide des Ressources numériques, dès lors que ces données relèvent : des opinions politiques (y compris l'appartenance syndicale), philosophiques ou religieuses, de la préférence sexuelle, de la santé (élargie aux données génétiques et biométriques), des infractions pénales et condamnations, des appréciations relatives aux difficultés sociales, de l'identification NIR (numéro de sécurité sociale).



A savoir : envoyer des données sensibles dans un service de stockage « cloud » tels que DROPBOX, One Drive, GOOGLE Apps, GMAIL, et iCloud et ou service de traitement ou diffusion « cloud » tels que SKYPE, HANGOUT, ou ILovePDF non mis à disposition par l'Etablissement représente un risque élevé de fuites de données. Il convient de s'interroger sur la nature sensible des contenus numériques manipulés et de proscrire le recours à ce type de services dès lors que ceux-ci ne pourraient être diffusés publiquement sans risquer de compromettre l'Etablissement.

2.7 Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer la continuité de service en cas d'absence ou de départ, l'agent de l'établissement prendra toute disposition utile pour permettre l'accès à ses données professionnelles aux personnes habilitées. De son côté le responsable hiérarchique, informé, prendra les dispositions nécessaires pour garantir la conservation de ces informations.



A savoir : Vous pouvez demander la création d'une boîte de messagerie fonctionnelle (par exemple directeur.dsi@uca.fr). Celle-ci sera ainsi consultable par plusieurs personnes en cas de votre absence et permettra d'assurer plus facilement la continuité de service.

3. Devoir d'information

3.1 Devoir d'information auprès de l'Établissement par les Usagers

Chaque Usager est tenu d'informer l'Établissement, lorsqu'il constate qu'une Ressource numérique, qu'elle lui ait été confiée ou non, fait l'objet d'une compromission avérée, suspectée ou potentielle, de façon à évaluer les mesures à prendre pour limiter les impacts sur le SI. Exemples :

- intrusion par un tiers,
- diffusion ou détournement d'un compte ou mot de passe,
- usurpation d'identité,
- faits de négligence, conduite à risque,
- vol ou perte d'un moyen d'identification (badge) ou d'un matériel, y compris les matériels personnels dans le cas où ces matériels sont utilisés pour accéder à des ressources numériques de l'établissement,
- duplication, téléchargement, divulgation non-autorisés,
- acte de piratage, infection par un virus informatique, fonctionnement douteux d'une ressource numérique,
- atteinte au droit d'auteur.

De même, un Usager qui prendrait conscience d'avoir réalisé un acte contraire à la charte générale est invité à en informer l'Établissement de façon à évaluer au plus tôt les mesures à prendre pour diminuer les impacts éventuels sur le Système d'Information.

3.2 Devoir d'information auprès des Usagers par l'Établissement

L'Établissement s'engage lorsqu'il en a connaissance à informer tout Usager dont les Ressources numériques ont fait l'objet d'un acte malveillant.

L'Établissement est soumis à des obligations légales en ce qui concerne l'utilisation de ses Ressources numériques. Notamment, l'Établissement est tenu d'enregistrer les accès aux Ressources numériques tierces via ses réseaux afin de s'assurer que ses propres Ressources informatiques ne soient pas utilisées à des fins illicites. Les données enregistrées peuvent être qualifiées de données à caractère personnel au sens de la loi du 6 janvier 1978 si les éléments enregistrés permettent d'identifier des personnes physiques.

Ces enregistrements sont conservés pour une durée d'un an. L'Établissement peut être amené à produire ces logs de connexion dans le cadre d'une réquisition judiciaire. En aucun cas l'Établissement n'accède à ces enregistrements pour ses besoins de gestion courants.

L'Etablissement se réserve la possibilité d'y accéder à titre exceptionnel lorsqu'il suspecte ou constate des cas de compromission et qu'il y va de la défense de ses intérêts propres ou de ceux de l'Usager. En dehors des cas susmentionnés, l'établissement s'interdit de consulter individuellement ces enregistrements et leur contenu.

Cette durée de conservation est limitative et ne peut excéder un an. De tels enregistrements existent également par défaut au sein de certaines applications logicielles et font partie intégrante des dispositifs de gestion et de sécurité mis en œuvre. Ces enregistrements peuvent être utilisés pour des besoins de gestion et d'administration : statistiques, débogage, protection contre la compromission, audit. En dehors de ces cas particuliers, l'Etablissement s'interdit de consulter individuellement ces enregistrements.

Enfin, la durée de conservation des données de travail à caractère personnel dans le système d'information se doit d'être compatible avec les missions de l'université et ses impératifs de gestion. Excepté pour les usagers de type intervenants invités qui entretiennent des relations à court terme avec l'établissement, les données à caractère personnel sont conservées dans les applications du système d'information tant qu'elles sont nécessaires à la gestion de leur dossier.

L'exploitation des données de travail à caractère personnel et des enregistrements se fait dans le respect de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Les usagers disposent d'un droit d'accès et de rectification qu'ils peuvent exercer auprès du CIL (Correspondant Informatique et Liberté) de l'établissement.

4. Surveillance du réseau et des Ressources informatiques

Pour assurer la meilleure sécurité informatique possible de l'Etablissement et une utilisation optimale des Ressources numériques par les Usagers, l'agent en charge de l'administration informatique est habilité à procéder à des vérifications régulières de la bonne utilisation de l'ensemble des postes et matériels informatiques, et plus généralement des Ressources numériques, confiés aux Usagers. Des statistiques d'utilisation pourront être établies et communiquées à la direction de l'Etablissement. A cet effet, l'Administrateur a mis en place des outils de surveillance de l'utilisation des Ressources numériques.

Toute mise en place de nouveaux outils de surveillance rendus nécessaires par l'évolution des besoins et des techniques sera précédée d'une information publiée sur l'intranet ou sur tout autre support en usage dans l'Etablissement. En outre, sur autorisation judiciaire préalable, l'Administrateur a la possibilité d'ouvrir les boîtes aux lettres et tous les fichiers, y compris personnels.

Il peut également faire consigner tout ordinateur (PC ou portable) et tout matériel et ainsi interdire momentanément l'utilisation d'un matériel mis à la disposition d'un Usager, et de fait, interdire l'accès à internet et au serveur de messagerie électronique.

Aucune exploitation des informations dont l'Administrateur réseau peut avoir connaissance dans l'exercice de ses fonctions ne saurait être opérée sur son initiative ni sous ordre hiérarchique, à des fins autres que celles liées au bon fonctionnement et à la sécurité des Ressources numériques.

5. Droit à la déconnexion

Dans le respect des principes énoncés à l'article L. 2242-8 du code du travail, l'établissement met en œuvre tous les dispositifs de régulation nécessaires pour assurer le droit à la déconnexion du personnel. Par ailleurs, une charte spécifique à la messagerie électronique est élaborée pour garantir le bon usage de cet outil.

6. Chartes spécifiques

Des chartes spécifiques à certaines ressources complètent la présente charte générale. Ces chartes spécifiques concernent des ressources à diffusion restreinte et ne s'adressent qu'aux utilisateurs habilités à utiliser ou accéder à ces ressources. Les Ressources numériques de l'Etablissement évoluant en permanence de même que les dispositions légales et réglementaires, en voici ci-dessous une liste non exhaustive :



Les Chartes

- Charte de messagerie
- Charte nomade
- Charte des Administrateurs techniques
- Charte d'hébergement
-

L'accès à des ressources à diffusion restreinte par un utilisateur habilité de l'Etablissement implique l'adhésion aux chartes spécifiques en vigueur. L'acceptation de la présente charte générale vaut acceptation de ce principe. Selon la criticité des Ressources numériques mises en jeu, l'Etablissement pourra recueillir une acceptation explicite en sus.

7. Exemples de pratiques contrevenant à la charte générale

L'utilisation des Ressources numériques mises à la disposition des Usagers par l'Etablissement est réputée loyale et rationnelle. Sans viser l'exhaustivité, ce chapitre illustre quelques situations propres au contexte universitaire qui contreviennent à la présente charte et en présence desquelles l'Etablissement ou toute autorité hiérarchique compétente peut prononcer des sanctions.

Sur le respect de la propriété intellectuelle et du droit d'auteur, et de la protection des données réputées confidentielles :

- Télécharger, détenir, utiliser ou diffuser des contenus média (musiques, films, livres) licenciés sans en avoir acquitté les droits ;
- Reproduire, diffuser des cours, des podcasts, des éléments pédagogiques sur des portails publics sans accord de leur auteur ;
- Télécharger, détenir, utiliser ou diffuser des logiciels licenciés sans en avoir acquitté les droits ;
- Divulguer ou s'exposer à la fuite de secrets de fabrique ou d'informations couvertes par le secret des affaires ;
- Divulguer, stocker ou transférer des données à caractère confidentiel sur des systèmes tiers tels que Dropbox, Gmail, Skype, etc.

Sur le respect mutuel des personnes : un Usager ne doit ni porter atteinte à la vie privée et à la personnalité de quiconque, ni nuire à l'activité professionnelle d'un Tiers par l'utilisation des Ressources numériques :

- Tenir des propos injurieux, racistes, menaçants, diffamatoires, harcelants, obscènes, pornographiques, sectaires, portant atteinte à l'intégrité morale ou à la dignité humaine, et plus généralement illégaux ;
- Usurper l'identité d'autrui, même sans dessein de lui nuire, ou utiliser intentionnellement le compte d'un autre Usager.

Sur le respect de l'intégrité des Ressources numériques : aucune atteinte aux dispositifs de protection ne doit être portée par l'Usager, aucune recherche sur la sécurité des systèmes d'information ne peut être effectuée sans autorisation préalable et l'information du RSSI (Responsable de la Sécurité des Systèmes d'Information):

- Altérer les dispositifs de sécurité déployés : désinstallation des logiciels antivirus, modification des paramétrages des mises à jour logicielles, entraver le déroulement des procédures automatisées, non-respect des consignes données par les administrateurs techniques ;
- Effectuer des tentatives répétées de connexion à des systèmes informatiques quels qu'ils soient et de façon mal intentionnée ;
- Développer, installer, copier des programmes visant à exploiter des failles de sécurité, à contourner la sécurité, à saturer des ressources informatiques, à enregistrer des actions sur un matériel à l'insu de l'utilisateur ;
- Envoyer massivement des courriels à des fins autres qu'institutionnelles et sans autorisation préalable de l'Etablissement ;
- Utiliser abusivement les listes de diffusion de la messagerie ;
- Relier aux réseaux privés (hors réseaux de nomadisme) de l'établissement un quelconque matériel externe non déclaré par l'Etablissement et sans autorisation préalable de l'Administrateur ;
- Installer, créer, configurer, maintenir un serveur d'information internet sans autorisation préalable (http, ftp, dns, dhcp, ...);
- Stocker des données, quels qu'en soient le volume et la nature, sur des supports externes hébergés par des Tiers, sans autorisation préalable de l'Administrateur ;
- Créer tout site internet accessible au public en ligne, ayant un lien direct ou indirect avec la Mission, sans information préalable de l'Etablissement s'agissant des Usagers étudiants, et sans l'autorisation préalable de l'Etablissement s'agissant des agents ;
- Accéder à des sites internet grâce aux outils de connexion et aux Ressources numériques mis à disposition par l'Etablissement, sans lien avec la Mission, de manière excessive dépassant la tolérance d'usage ;
- Participer à des forums en ligne ou accéder à des réseaux sociaux, en divulguant des informations inadéquates ou susceptibles de porter atteinte à la réputation de l'Etablissement, de toute personne ou de tout organisme, de violer le secret des correspondances ou la confidentialité de programmes de recherche ;
- Se déplacer munis d'ordinateur(s) portable(s) ou de support(s) amovible(s) confié(s) par l'Etablissement ou comportant des informations et données de l'Etablissement, sans prendre les précautions d'usage, à savoir : la conservation permanente sous contrôle, l'utilisation sans risque de divulgation d'information, le respect des règles d'hygiène informatique (écran de veille, codes d'accès, mise sous clé, chiffrement des données), la suppression de toutes données sensibles ou confidentielles avant tout déplacement à l'étranger.

8. Les sanctions et les textes de référence

8.1 Sanctions

L'établissement peut en cas de manquement grave aux règles et obligations définies dans la charte, pour tout Usager :

- ➔ Interdire provisoirement à titre conservatoire l'accès aux ressources numériques ;
- ➔ Déclencher des procédures disciplinaires et/ou pénales.

8.2 Principaux textes législatifs et sanctions se rapportant à la sécurité des systèmes d'information et à la protection des personnes

Sur la protection des personnes :

- Directive européenne 2002/58/CE du 12 juillet 2002 sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;
- Convention Européenne du 28 janvier 1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel ;
- Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi 2004-801 du 06 août 2004 ;
- Article 226-24 du Code Pénal : responsabilité des personnes morales des infractions aux dispositions de la loi sur les atteintes à la personnalité.

Sur la propriété intellectuelle :

- Article 335-2 du code de la Propriété intellectuelle : répression de la contrefaçon (jusqu'à 3 ans de prison et 300 000 Euros d'amende) ;
- Article 122-6 du code de la Propriété intellectuelle Sur l'atteinte aux droits de la personne résultant de fichiers ou traitements informatiques ;
- Articles 226-16 et suivants du Code pénal : violations de la Loi « Informatique et libertés » (jusqu'à cinq ans de prison et 300.000 € d'amende).

Sur les atteintes aux systèmes de traitement automatisé de données :

- Article 323-1 et suivants du code pénal: introduction frauduleuse, modification, suppression de données dans un système d'information ainsi que extraction, détention, reproduction ou transmission frauduleuse de données (cinq ans de prison et 75000 euros d'amende voire 7 ans et 100000 euros s'il s'agit de données à caractère personnel) ;

- Directive de la C.E.E. du 21 décembre 1988 sur l'harmonisation de la protection des logiciels.

Sur la violation des secrets et la prise de nom d'un tiers :

- Article 410-1 et 411-6 du nouveau Code Pénal : intérêts fondamentaux de la nation, secrets économiques et industriels ;
- Article 432-9 alinéa 1 et 226-15 du nouveau Code pénal: secret des correspondances (3 ans de prison et 45 000 Euros d'amende) ;
- Article 434-23 du Code pénal : usurpation d'identité (5 ans et 75 000 Euros d'amende) ;
- article 621-1 de la Propriété intellectuelle : secrets de fabrique (2 ans de prison et 30 000 Euros d'amende).

9. Diffusion et révision de la charte générale

Les technologies de l'information et leur cadre législatif évoluent fortement. L'Etablissement révisera dès lors que nécessaire la présente charte générale. Il s'engage à porter à la connaissance des Usagers toute révision de celle-ci au moyen des communications électroniques ou des portails intranet.

La présente charte reste annexée au règlement intérieur de l'Etablissement et consultable sur simple demande auprès de la Direction Générales des Services.

Toute information complémentaire peut être obtenue auprès de :

- la direction des systèmes d'information (DSI) ;
- le responsable de la sécurité des systèmes d'information (RSSI) ;
- le correspondant informatique et libertés (CIL) ;
- la direction des affaires juridiques (DAJ).