Institut de Chimie de Clermont-Ferrand
ICCF - UMR 6296

REGLEMENT INTERIEUR

de

l'ICCF
UMR 6296

Chimie 7 - 24, avenue Blaise Pascal, TSA 60026 CS 60026, 63178 AUBIERE Cedex – France
☎ : (33) 04 73 40 71.25
: direction.iccf@uca.fr https://iccf.uca.fr/

PREAMBULE

L'Unité 6296 (ci-après désignée l'« Unité ») est une *UMR* implantée dans les locaux de l'Université Clermont Auvergne

Le présent règlement intérieur a été soumis à l'avis du Conseil de laboratoire*,* réuni le 13 avril 2017.

Il a pour objet de préciser notamment l'application dans l'Unité :

- de son organisation générale,
- des règles générales et permanentes relatives au temps de travail (horaires, congés …), à l'utilisation des locaux et du matériel,
- de la règlementation en matière de santé et de sécurité au travail,
- de la réglementation en matière de sécurité de l'information et des systèmes d'information,
- des dispositions relatives à la protection du potentiel scientifique et technique (PPST).

Le présent règlement intérieur est complémentaire à celui de l'Université Clermont Auvergne. En cas de contradiction, les dispositions les plus restrictives prévaudront.

Toute modification sera soumise à l'avis du Conseil de laboratoire *(ou de l'Assemblée Générale)* et devra faire l'objet le cas échéant d'un avenant ou d'un nouveau règlement intérieur.

Il s'applique à l'ensemble du personnel affecté à l'Unité, y compris les agents non titulaires et les stagiaires.

Toute évolution de la réglementation applicable dans les établissements tutelles de l'Unité s'applique de fait à l'Unité, même si le présent règlement intérieur n'en fait pas état.

SOMMAIRE

1 – Fonctionnement général de l'unité :

1.1 Le Conseil de Laboratoire

Composition et fonctionnement

Sa composition et ses modalités de fonctionnement sont prévues en application de la décision CNRS n° 920368SOSI du 28/10/1992.
Il est présidé par le Directeur de l'Unité. Il est composé de 13 membres élus par collège et s/collège selon un mode de scrutin plurinominal à 2 tours: (6 membres pour le s/collège enseignants-chercheurs, 3 membres pour le s/collège chercheurs, 1 membre pour le s/collège doctorants, 3 membres pour le collège ITA/BIATSS), 5 membres nommés, 2 membres invités permanents qui n'ont pas le droit de vote (1 Agent de Prévention référent, 1 gestionnaire référent), le Directeur, le Directeur-adjoint. Les membres ne peuvent pas se faire remplacer mais ils peuvent donner leur procuration à un membre de leur collège. Un membre du conseil ne pourra avoir qu'une seule procuration.
Il a un rôle consultatif et émet un avis sur toutes les questions relatives à la politique scientifique, la gestion des ressources, l'organisation et le fonctionnement de l'Unité.
Le conseil se réunira au moins 3 fois/an. Les membres seront informés de la tenue des réunions par e-mail et recevront une convocation. La durée de son mandat est de 5 ans.

Compétences

Le Conseil de laboratoire a un rôle consultatif. Il est consulté par le Directeur de l'Unité sur :
- l'état, le programme, la coordination des recherches, la composition des équipes ;
- les moyens budgétaires à demander par l'Unité et la répartition de ceux qui lui sont alloués ;
- la politique des contrats de recherche concernant l'Unité ;
- la politique de transfert de technologie et la diffusion de l'information scientifique de l'Unité ;
- la gestion des ressources humaines ;
- la politique de formation par la recherche ;
- les conséquences à tirer de l'avis formulé par la ou les sections du Comité national de la recherche scientifique dont relève l'Unité ;
- le programme de formation en cours et pour l'année à venir ;
- toutes mesures relatives à l'organisation et au fonctionnement de l'Unité et susceptibles d'avoir une incidence sur la situation et les conditions de travail du personnel.

Le directeur de l'Unité peut en outre consulter le conseil de laboratoire sur toute autre question concernant l'Unité.

En application de l'article 241-1 du décret n°83-1260 du 30 décembre 1983 modifié, le Conseil de laboratoire est consulté préalablement à l'établissement du rapport de stage des fonctionnaires nommés dans les corps d'ingénieurs, de personnels techniques et d'administration (ITA) de la recherche.

En application de l'article 18 du décret n°82-993 du 24 novembre 1982 modifié, l'avis du Conseil de laboratoire est recueilli en vue de la nomination du Directeur de l'Unité.

Lorsque l'Unité est évaluée par une ou plusieurs sections du Comité national de la recherche scientifique, le Conseil de laboratoire joint au dossier un rapport pouvant comporter ses observations à l'adresse de la (des) section(s).

Le Conseil de laboratoire est tenu informé par le Directeur de l'Unité de la politique du ou des instituts du CNRS, ainsi que des politiques scientifiques des autres établissements de tutelle de l'Unité et de leur incidence sur le développement de l'Unité

1.2 L'Assemblée Générale

Elle comprend tous les personnels de l'Unité. Elle est réunie dans les conditions suivantes : 1 fois par an et pour réunions extraordinaires pouvant être provoquées soit par la direction, soit par au moins un tiers des personnels électeurs du Conseil de Laboratoire.

1.3 Le Conseil Scientifique

Il comprend le Directeur, le Directeur-adjoint, les responsables d'équipes, le coordinateur des Services Techniques et Appui à la Recherche, les responsables de thématiques, les responsables d'axes, un représentant de l'Université Clermont Auvergne (UCA), un représentant du CNRS, un représentant de SIGMA Clermont, 2 représentants des ITA/BIATSS, 1 représentant des contractuels chercheurs. Des membres extérieurs au Conseil Scientifique pourront être invités selon l'ordre du jour. En cas d'indisponibilité, les membres peuvent se faire remplacer. Les remplaçants peuvent voter à condition d'être porteurs d'une seule procuration. Le conseil se réunira au moins 3 fois/an.

1.4 Le Comité de Direction

Il comprend le Directeur, le Directeur adjoint, les responsables d'équipes et le coordinateur des Services Scientifiques Techniques et Administratifs de la Recherche (SSTAR). Il se réunit avec une fréquence hebdomadaire.

1.5 La Commission spéciale Hygiène et Sécurité

Il se compose d'un Président : Directeur de l'ICCF ; d'un secrétaire : Assistant de Prévention référent ; d'invités : Ingénieurs Hygiène et sécurité de l'UCA et du CNRS et du conseiller de prévention de SIGMA Clermont ; des Assistants de Prévention de l'ICCF, d'un Correspondant Environnement, du responsable Qualité, des membres de droit : Médecin de prévention personnel UCA, Médecin de prévention personnel CNRS et des représentants du Personnel (un ITA/BIATSS, un personnel chercheur, un personnel enseignant chercheur, un contractuel chercheur, ..). La commission se réunira au moins 1 fois/an.

2 – Vie du laboratoire :

L'ensemble du personnel permanent ou contractuel contribue aux activités de recherche de l'unité. Il est également impliqué dans les activités annexes du laboratoire : séminaires, charges collectives, relations avec des collaborateurs (académiques ou industriels), encadrement, mise à jour du site web, animations scientifiques.

2.1 – Arrivée d'un personnel

Le responsable d'équipe, l'assistant de prévention du bâtiment doivent être avertis de l'accueil de tout nouvel arrivant (doctorant, post-doctorant, stagiaire, professeur invité, nouveau personnel permanent) afin de planifier son accueil en tenant compte des capacités des locaux et des moyens logistiques de l'équipe. Tout nouvel arrivant non permanent doit être pris en charge par un encadrant permanent. Pour les démarches inhérentes à l'accueil d'une personne, il faut se référer aux procédures d'accueil (Annexe n°1).

2.2 – Départ d'un personnel

En cas de départ définitif d'un personnel, celui-ci devra restituer les éléments qui lui auront été confiés (clés, carte magnétique, cahiers de laboratoire, matériel de laboratoire, EPI, …).

3 – Temps de travail, horaires, congés, absences

3.1 – Temps de travail

Pour les personnels CNRS (chercheurs et ITA) : la durée annuelle de travail est fixée à 1607 heures. Cette durée tient compte des 7 heures de travail dues au titre de la journée de solidarité.
Les modalités de mise en œuvre dans l'Unité prennent en compte les dispositions du décret n°2000-815 du 25 août 2000 modifié et de son arrêté d'application du 31 août 2001 ainsi que celles du cadrage national du CNRS en date du 23 octobre 2001 modifié.

Pour les personnels BIATSS de l'UCA : la durée annuelle de travail effectif est de 1593 heures. Pour toutes les questions relatives au temps de travail, aux principales règles concernant les obligations de service et les congés légaux, se rendre sur l'ENT->com'interne->espace des personnels->GRH.

Pour les CDD, il faut se référer au contrat de travail.

La durée hebdomadaire du travail effectif pour chaque agent de l'Unité travaillant à plein temps est :

- Pour le personnel permanent et contractuel CNRS
  - 38 heures 30 sur cinq jours
- Pour le personnel technique UCA :
  - 37 heures 30 sur cinq jours pour l'ensemble des agents titulaires
  - les agents contractuels doivent se référer à leur contrat de travail.
- Pour le personnel technique SIGMA Clermont :
  - 37 heures 40 sur cinq jours.

Les personnels autorisés à accomplir un service à temps partiel d'une durée inférieure ou égale à 80 % peuvent travailler selon un cycle hebdomadaire inférieur à 5 jours, en accord avec les différentes tutelles, sous réserve d'organisation de services.

Pour les enseignants-chercheurs de l'UCA et de SIGMA Clermont : la durée annuelle est de 1607 heures en référence au Décret n°84-431 du 6 juin 1984 fixant les dispositions statutaires communes applicables aux EC.

La durée de travail effectif est organisée du lundi au vendredi.

3.2 – Horaires journaliers, ouverture du laboratoire, accès aux locaux

Les horaires d'ouverture du laboratoire se situent entre 7h30 et 19h30 du lundi ou vendredi. Le temps de travail quotidien de chaque agent ne peut excéder 11 heures. Pour accéder aux locaux en dehors des plages horaires spécifiées ici, l'ensemble du personnel doit respecter les consignes indiquées dans la charte d'Hygiène et Sécurité jointe en annexe (Annexe n°2). Pour les stagiaires et étudiants, en cas d'absence de l'encadrant, celui-ci doit s'assurer qu'au moins un permanent est en mesure d'encadrer le personnel présent, sinon l'activité doit être stoppée.

Le temps de travail correspond à un temps de travail "effectif". Il ne prend pas en compte la pause méridienne obligatoire qui ne peut être ni inférieure à 45 minutes ni supérieure à 2 heures. Aucun temps de travail quotidien ne peut atteindre 6 heures sans que les agents bénéficient d'un temps de pause d'une durée minimale de 20 minutes.

3.3 – Travail isolé

Les situations de travail isolé en dehors des heures ouvrables doivent rester exceptionnelles et être gérées de façon à ce qu'aucun agent ne travaille seul en un point où il ne pourrait être secouru à bref délai en cas d'accident. En dehors des heures ouvrables, le travail isolé est soumis à l'autorisation exceptionnelle du responsable de thématique et de l'AP du bâtiment qui en informent le Directeur dans un délai d'une semaine. Le Directeur valide ou non la demande par écrit. Le personnel ayant obtenu l'autorisation exceptionnelle devra se munir de l'appareil de Protection Travailleur Isolé (PTI). Un PTI est disponible par bâtiment.

3.4 – Congés annuels

Les périodes de fermeture de l'unité sont conformes aux dates de fermeture définies par l'Université Clermont Auvergne. Sous condition des nécessités de service et après accord du directeur d'Unité, certains personnels peuvent travailler exceptionnellement pendant cette période, après avoir obtenu une dérogation du Directeur Général des Services de l'université.

Les jours de congés sont accordés, après en avoir informé son responsable hiérarchique, sous réserve des nécessités de service.

- Personnels BIATSS de l'UCA titulaires:

Le nombre de jours de congés annuels est fixé à 49 jours par année universitaire (45 jours moins 1 jour de solidarité au titre des congés annuels et 5 jours de congés supplémentaires au titre de l'Aménagement et Réduction du Temps de Travail (ARTT). Pour les personnels contractuels recrutés sur contrat à durée déterminée inférieure ou égale à 10 mois, le droit aux congés est de 2,5 jours par mois de travail.

- Personnels ITA et chercheurs CNRS titulaires :

Le nombre de jours de congés est de 45 jours ouvrés moins 1 jour de solidarité par année civile. Il prend en compte le nombre de jours de congés annuels et les jours de congés accordés au titre de l'Aménagement de la Réduction du Temps de Travail (jours RTT) compte tenu de la durée hebdomadaire du travail. Les personnels peuvent bénéficier de deux jours de fractionnement des congés annuels : 1 jour si l'agent prend 5,6 ou 7 jours en dehors de la période du 1er mai au 31 octobre et de 2 jours si ce nombre est au moins égal à 8 jours. Les jours RTT sont utilisés dans les mêmes conditions que les jours de congés annuels.

Les congés sont obligatoirement pris au minimum par demi-journée.

Le report des jours de congés annuels ainsi que les jours RTT non utilisés, est autorisé jusqu'à la date définie par la tutelle dont les agents dépendent. Les jours qui n'auront pas été utilisés à cette date seront définitivement perdus, sauf si ces jours ont été déclarés dans un Compte Epargne Temps (CET).

3.5 - Compte-épargne temps

Les modalités sont définies par le décret 2009-1065 du 28 août 2009 modifiant certaines dispositions relatives au CET dans la fonction publique d'Etat et dans la magistrature et arrêté du 28 août 2009 pris pour application du décret n°2002-634 du 29 avril 2002 modifié pour la mise en œuvre au CNRS et dans la circulaire n° 2010-205 du 17 septembre 2010 parue au bulletin officiel du 4 novembre 2010 à l'UCA.

3.6 Durée des absences de service pour congés

L'absence de service ne peut excéder 31 jours consécutifs (la durée des congés est calculée du premier au dernier jour sans déduction des samedis, dimanches et jours fériés).

3.7 Suivi des congés

Afin de pouvoir adapter l'organisation du travail, chacun doit effectuer ses demandes de congés, dans la mesure du possible, avec un délai de prévenance de 10 jours. Les personnels CNRS (titulaires et contractuels) doivent déposer leurs congés dans l'application AGATE. Les BIATSS de l'UCA doivent déposer leurs congés via leur ENT.

Le suivi des congés (annuels et RTT) est réalisé dans l'Unité sous la responsabilité du Directeur, et transmis à la délégation (notamment pour la mise en œuvre du CET pour les CNRS).

- Personnels BIATSS ou en CDD de SIGMA Clermont

Les congés de ces personnels sont gérés par la DRH de SIGMA Clermont.

- Enseignants-chercheurs de l'UCA et de Sigma Clermont

En l'absence de textes officiels régissant les congés des enseignants-chercheurs, la direction de l'ICCF demande aux enseignants-chercheurs de déclarer leurs jours de congés à l'aide de la fiche de congés disponible sur le site web de l'ICCF.

3.8 – Absence :

Absence pour raison médicale :

Toute indisponibilité consécutive à la maladie doit, sauf cas de force majeure, être dûment justifiée et signalée au responsable de l'Unité dans les 24 heures. Le salarié doit produire un certificat médical indiquant la durée prévisible de l'indisponibilité dans les 48 heures qui suivent l'arrêt de travail.
Tout accident corporel survenant dans le cadre de l'activité professionnelle sera immédiatement déclaré à l'employeur et à l'assistant de prévention et noté dans le registre Hygiène et Sécurité (cf Rubrique Hygiène et Sécurité).

Autorisations d'absence pour garde d'enfant

Pour les personnels CNRS et UCA, les autorisations d'absence pour garde d'enfant (12 jours ou 6 jours si le conjoint en bénéficie) doivent être signalés le jour même au secrétariat et être justifiés par un certificat médical sinon l'agent devra déposer un jour de congé. Les personnels BIATSS devront également faire une demande auprès de l'UCA (formulaire disponible sur l'ENT). Les personnels SIGMA Clermont doivent s'adresser à leur DRH.

Missions

Tout agent se déplaçant pour l'exercice de ses fonctions doit être en possession d'un ordre de mission établi préalablement au déroulement de la mission. Celui-ci doit être dûment rempli et remis au directeur pour signature. La procédure et les délais prévus par l'administration doivent impérativement être respectés. Ce document est obligatoire du point de vue administratif et juridique ; il assure la couverture de l'agent au regard de la réglementation sur les accidents de service. La règlementation impose l'autorisation préalable du Fonctionnaire Sécurité Défense pour les missions des agents dans certains pays étrangers.

L'agent amené à se rendre directement depuis son domicile sur un lieu de travail occasionnel, sans passer par sa résidence administrative habituelle, est couvert en cas d'accident du travail sous réserve d'être en possession d'un ordre de mission au départ et retour de la résidence familiale.

Dans l'hypothèse où l'agent utilise un véhicule administratif ou son véhicule personnel, le Directeur de l'Unité doit avoir donné préalablement son autorisation.

Les consignes sur les ordres de missions CNRS, UCA et SIGMA Clermont sont consultables sur le site internet du laboratoire (rubrique Vie du laboratoire, missions).

4 – Résultats scientifiques :

4.1 – Confidentialité :

Les travaux de l'Unité constituent par définition des activités confidentielles (cf. Flash n° 32 – Avril 2017 du Ministère de l'Intérieur sur l'Ingérence économique, disponible sur http://www.prefectures-regions.gouv.fr/ile-de-france). Par conséquent, les personnels de l'Unité sont tenus de respecter la confidentialité de toutes les informations de nature scientifique, technique ou autre, quel qu'en soit le support, ainsi que de tous les produits, échantillons, composés, matériels biologiques, appareillages, systèmes logiciels, méthodologies et savoir-faire ou tout autre élément ne faisant pas partie du domaine public dont ils pourront avoir connaissance du fait de leur séjour au sein de l'Unité, des travaux qui leur sont confiés ainsi que de ceux de leurs collègues. Cette obligation de confidentialité reste en vigueur tant que ces informations ne sont pas dans le domaine public. Ce principe de confidentialité continue à s'appliquer lorsque les agents ont quitté le laboratoire.

4.2 – Production scientifique

Les chercheurs doivent se référer au guide du CNRS intitulé « Pratiquer une recherche intègre et responsable » disponible sur http://www.cnrs.fr/comets/spip.php?article145.

Les publications des membres de l'Unité doivent faire apparaître l'appartenance à l'Unité et le rattachement aux tutelles sous la forme :

X. Dupont
Université Clermont Auvergne, CNRS, SIGMA Clermont, Institut de Chimie de Clermont-Ferrand, F-63000 Clermont–Ferrand, France.

Doivent être exclues les mentions à des sous-structures (équipes,…).

Toutes les publications (ACL, conférences, communications orales, posters, chapitres d'ouvrages, séminaires, articles de vulgarisation, thèses…) dont tout ou partie du travail a été effectuée à l'Unité doivent être signalées au secrétariat.

4.3 – Communication :

Les travaux et les projets de recherche développés au sein de l'ICCF (rapports, thèses, conférences, flyers, posters, …) doivent mentionner obligatoirement l'ICCF (intitulé, sigle, logo).

Il est vivement recommandé d'utiliser les templates de l'ICCF dans les présentations de communications orales et les posters.

Le contenu du site internet du laboratoire est sous la responsabilité du Directeur.

5 – Hygiène et sécurité :

Chaque personnel permanent ou non permanent s'engage à lire et à signer la Charte Hygiène et Sécurité jointe au présent règlement intérieur (Annexe n°2).

Les questions relatives à l'hygiène et la sécurité de l'unité sont discutées lors des commissions Hygiène et Sécurité et les décisions validées en conseil de laboratoire.

S'il incombe au Directeur de veiller à la sécurité et à la protection des personnels et d'assurer la sauvegarde des biens de l'Unité, chacun doit se préoccuper de sa propre sécurité et de celle des autres.

Les Assistants de Prévention (AP) assistent et conseillent le Directeur et les responsables d'équipes, ils informent et sensibilisent les personnels travaillant dans l'Unité pour la mise en œuvre des consignes d'hygiène et sécurité.

L'institut dispose d'un AP par bâtiment dont un AP référent, de 2 PCR (Personnes Compétentes en Radioprotection), 1 PCR en source scellée et 1 PCR en source non scellée et d'un référent Laser. Les informations Hygiène et Sécurité sont disponibles à chaque étage des bâtiments et sur le site web.

Les dispositions à prendre en cas d'accident et d'incendie font l'objet d'un document spécifique et sont affichées à chaque étage des bâtiments occupés par l'Unité.

Un registre Santé et Sécurité au Travail dans lequel les personnels doivent consigner tous les incidents et accidents survenus dans le laboratoire ainsi que leurs observations et suggestions relatives à la prévention des risques et à l'amélioration des conditions de travail est disponible au secrétariat de l'unité. Les déclarations se font à l'aide des formulaires disponibles sur le site web (http://iccf.univ-bpclermont.fr/spip.php?article647) et doivent être transmises à l'AP du bâtiment.

Les Assistants de Prévention doivent fournir aux personnels, dès leur arrivée, la formation et les informations nécessaires à l'accomplissement de leur travail et au respect des consignes générales de sécurité. Tout travail expérimental ne pourra démarrer sans la formation au poste de travail.

En respect du code du travail, il est interdit aux personnels de fumer sur les lieux de travail (Décret ° 92-478 du 29 mai 1992). En application de l'article L.3511.7.1 du code de la santé publique (loi n°2016-41 du 26 janvier 2016), il est interdit de vapoter dans les lieux de travail fermés et couverts à usage collectif.

L'introduction d'animaux domestiques dans les locaux est strictement interdite.

Il est interdit de pénétrer ou de demeurer dans l'Unité en état d'ébriété (Article R4228-20 du code du travail).
La consommation de boissons alcoolisées dans les locaux de travail est interdite sauf autorisation exceptionnelle du Directeur de l'Unité et sous couvert de l'hébergeur.

Le Directeur d'Unité doit retirer de son poste de travail toute personne en état apparent d'ébriété.

L'accès à l'ICCF est uniquement autorisé aux personnes exerçant une activité professionnelle en relation avec l'Institut. Tous les locaux de recherche, en dehors des bureaux, possèdent une "fiche réflexe" et/ou une signalétique particulière qui est affichée sur leur porte ou immédiatement à proximité. Leur accès est réglementé de la façon suivante : seules les personnes autorisées ont accès à ces locaux, les autres personnes doivent être accompagnées.

Le transport de marchandises (matières premières, échantillons, produits de synthèse, toute matière issue de l'activité scientifique de l'Institut, matériel scientifique …) fait l'objet d'une réglementation complexe et exigeante (cf Charte Hygiène et Sécurité Annexe 2). Pour les envois de marchandises, il faut d'adresser aux « correspondants achats » des équipes ou au secrétariat de l'ICCF.

La rédaction du Document Unique de l'Unité est obligatoire depuis le 5 novembre 2001. Selon l'article Article R. 4121-1 du code du travail (ancien article: R 230-1), « l'employeur transcrit et met à jour dans un document unique les résultats de l'évaluation des risques pour la santé et la sécurité des travailleurs à laquelle il procède. » Ce document a pour objectif d'améliorer les conditions de travail et la santé au travail, en diminuant les accidents du travail et les maladies professionnelles.
L'inventaire des risques est réalisé, par l'employeur pour chaque unité de travail, en repérant les situations à risques. Les risques sont évalués par leur gravité et leur probabilité afin de définir les plus importants et de les traiter en priorité. Seuls les risques effectivement présents doivent figurer dans ce document.
La mise à jour annuelle de ce document permet la mise en place d'un « Plan de Prévention de l'Institut» pour l'année en cours. Il est mis à disposition, sous forme papier ou numérique, aux personnes suivantes (selon le décret 2008-1347 du 17 décembre 2008):

- des travailleurs de l'Unité;
- des membres du comité d'hygiène, de sécurité et des conditions de travail ou des instances qui en tiennent lieu ;
- des délégués du personnel ;
- du médecin du travail ;
- des agents de l'inspection du travail ;
- des agents des services de prévention des organismes de sécurité sociale ;
- des agents des organismes professionnels de santé, de sécurité et des conditions de travail mentionnés à l'article L. 4643-1 ;
- des inspecteurs de la radioprotection mentionnés à l'article L. 1333-17 du code de la santé publique et des agents mentionnés à l'article L. 1333-18 du même code, en ce qui concerne les résultats des évaluations liées à l'exposition des travailleurs aux rayonnements ionisants, pour les installations et activités dont ils ont respectivement la charge.

6 – Démarche Qualité de l'ICCF

La direction de l'Institut définit une politique qualité et la met en œuvre *via* une cellule qualité. Cette dernière est composée d'un responsable et au minimum d'un "référent qualité" par équipe. Des cahiers de laboratoire sont à la disposition du personnel au secrétariat de l'unité. Un cahier de laboratoire est remis à tout nouvel arrivant.

7 – Formation

7.1 Plan de formation des personnels

Le plan de formation de l'Unité est soumis pour avis au conseil d'Unité avant l'envoi au CNRS. Les correspondants formation de l'Unité informent et conseillent les personnels pour leurs besoins et demandes de formation. Le correspondant référent participe, auprès du Directeur d'Unité, à l'élaboration du plan de formation de l'Unité.

7.2 Formation par la recherche

L'encadrement des stagiaires par un agent titulaire ou non de l'Unité est soumis à l'autorisation préalable du responsable d'équipe ou du Directeur de l'Unité. Tout stage effectué en partie au laboratoire doit faire l'objet d'une convention de stage tripartite signée par le stagiaire avec les tutelles concernées, avant le début du stage.
Les doctorants doivent signer la charte des thèses prévues par l'Ecole Doctorale de rattachement.

8 – Utilisation des moyens informatiques

L'utilisation des moyens informatiques est soumise à des règles explicitées dans la charte informatique de l'Université Clermont Auvergne (Annexe n°3). Cette charte a pour objet de préciser la responsabilité des utilisateurs, en accord avec la législation et doit être signée par tout nouvel arrivant. Cette charte informatique est annexée au présent règlement intérieur.

Le CSSI (Chargé de la Sécurité des Systèmes d'Information) assiste et conseille le Directeur d'Unité dans l'élaboration du plan d'action de mise en œuvre de la Politique de Sécurité des Systèmes d'Information (PSSI) opérationnelle de l'Unité et du suivi de sa mise en œuvre. Il informe et sensibilise les personnels travaillant dans l'Unité pour la mise en œuvre des consignes de sécurité des systèmes d'information. Il est le point de contact pour la signalisation des incidents de sécurité des Systèmes d'Information (SI) qui concernent le personnel et les systèmes d'information de l'Unité et remonte les incidents à la chaîne fonctionnelle de Sécurité des systèmes d'information (SSI) décrite par la PSSI opérationnelle de l'Unité.

9 – Utilisation des ressources techniques collectives

Les membres de l'Unité ont accès aux services suivants, conformément à leur propre réglementation :

- Accès à la BCU
- Accès à la Bibliothèque de chimie
- Accès aux bases de données
- Services communs de l'ICCF
- Services d'UCA-START

10 - Procédure de révision du règlement

Le règlement intérieur est soumis pour signature par le Directeur d'Unité aux tutelles d'appartenances, après avis du Conseil d'Unité.

Des modifications ou adjonctions à ce règlement pourront être proposées par le Directeur ou le Conseil d'Unité après inscription à l'ordre du jour. Leur adoption doit être approuvée par vote par la majorité des membres du Conseil. Toute proposition de modification rejetée par le Conseil d'Unité ne pourra être soumise à nouvelle discussion avant un délai de six mois.

Le présent règlement sera affiché dans les locaux de l'unité. Il sera transmis, pour information au Directeur Général Adjoint du CHU de Clermont-Ferrand (partenaire associé) en charge de la recherche clinique et l'innovation. Il sera aussi transmis à tous les personnels et usagers du laboratoire, ainsi qu'aux nouveaux entrants.

Fait à Aubière, le 31 JAN. 2019

Pour l'ICCF – UMR 6296

Institut de Chimie de Clermont-Ferrand ICCF UMR 6296

Fabrice LEROUX
Directeur

Pour l'Université Clermont Auvergne

UCA Université Clermont Auvergne

Mathias BERNARD
Président

Pour SIGMA Clermont

SIGMA CLERMONT CAMPUS DES CÉZEAUX Tél. 04 73 28 80 00 CS 20265 - 63178 AUBIERE CEDEX

Sophie COMMEREUC
Directrice

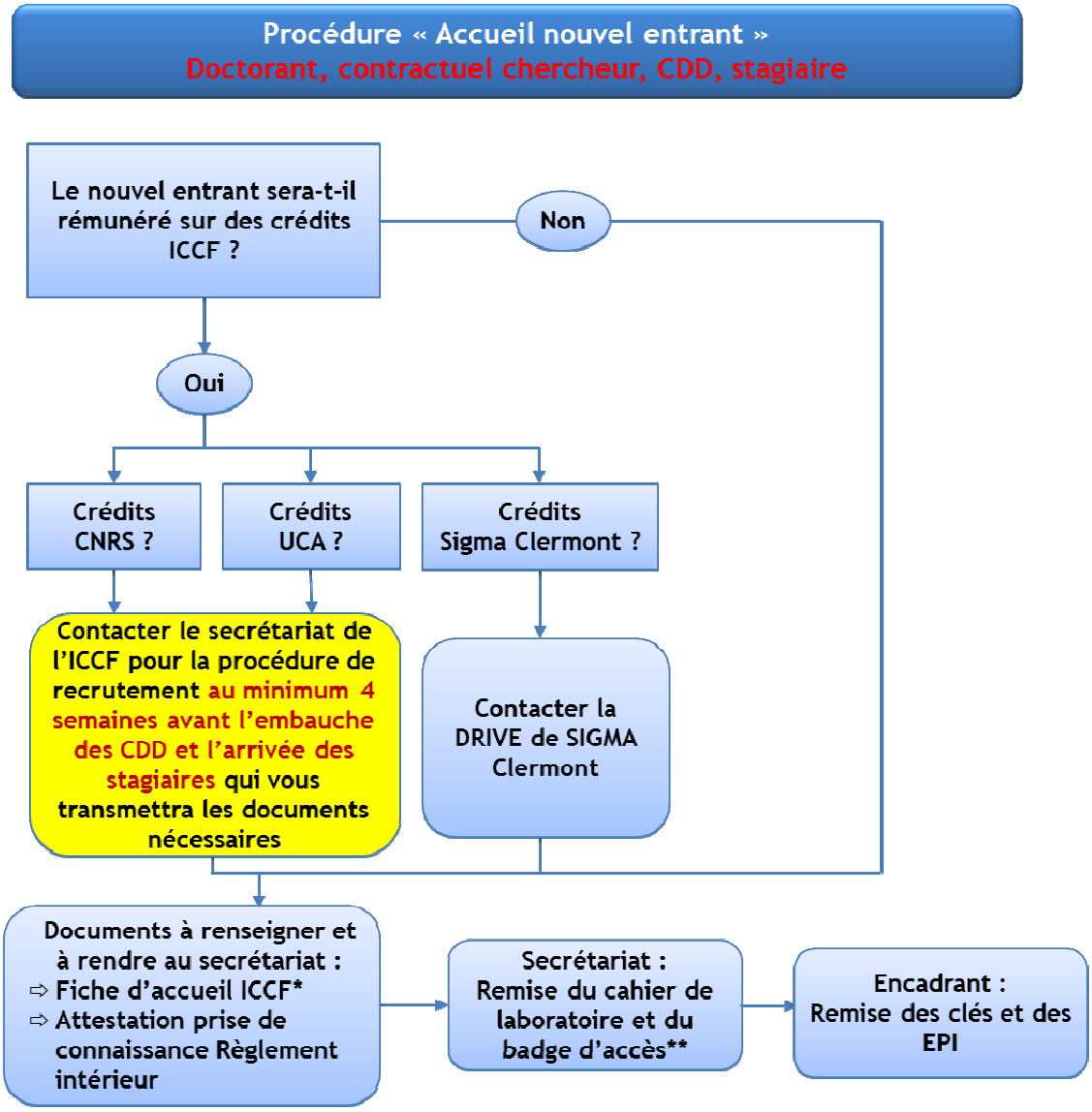
Pour le CNRS, le 07.02.2019

Frédéric FAURE
Délégué Régional
CNRS Rhône Auvergne

Frédéric FAURE
Délégué Régional

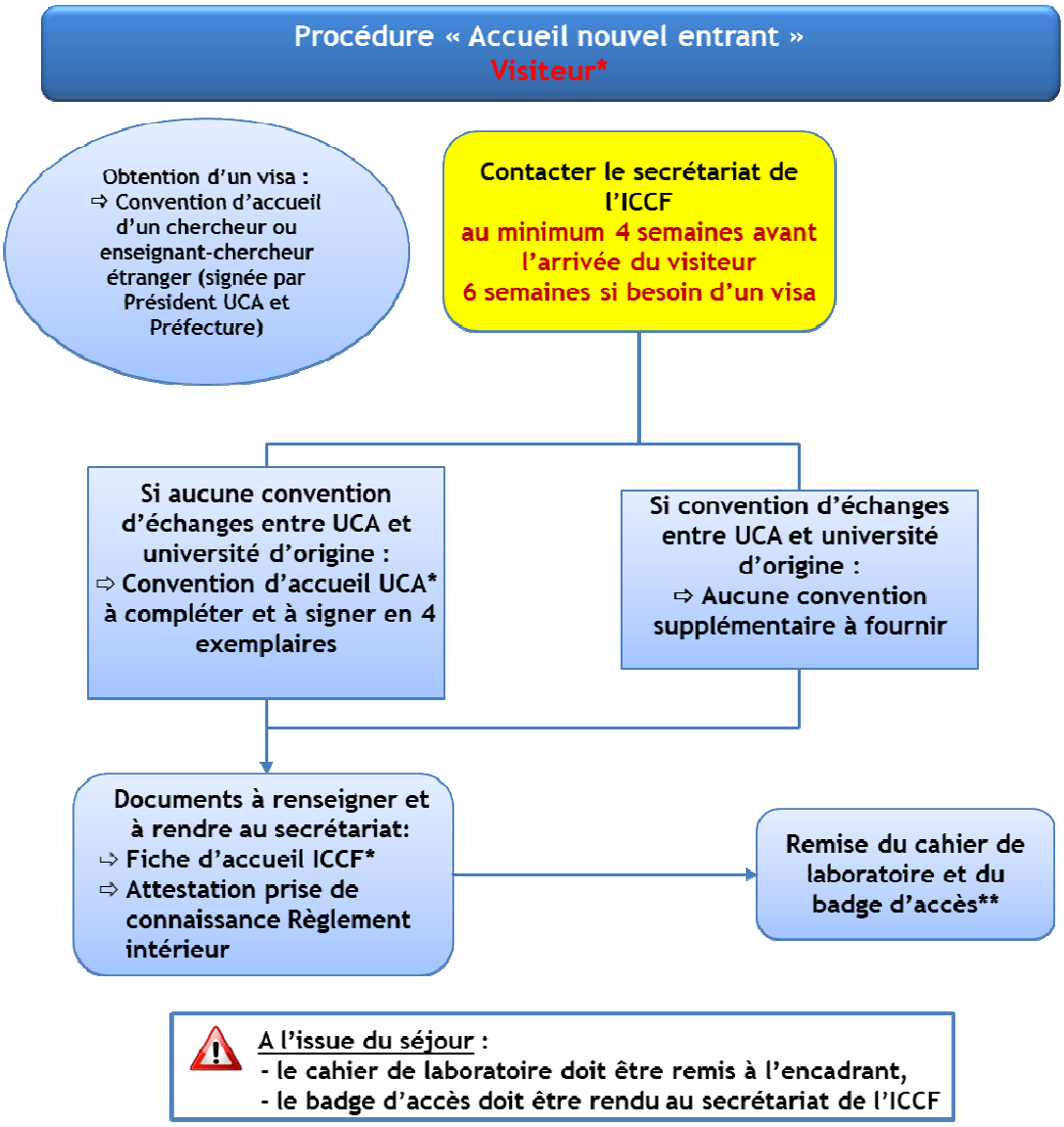
Annexe n°1

Procédures d'accueil



⚠ A l'issue du séjour :
- le cahier de laboratoire doit être remis à l'encadrant,
- le badge d'accès doit être rendu au secrétariat de l'ICCF

**** Disponible sur le site internet de l'ICCF, à la rubrique « Vie du laboratoire/Documents utiles ».***
***** Les personnels dont le séjour à l'ICCF serait inférieur à 1 mois et les stagiaires qui ne sont pas en stage à temps plein à l'ICCF n'auront pas de badge.***



Ne concerne pas les PR invités par l'UCA

****Disponible sur le site internet de l'ICCF, à la rubrique « Vie du laboratoire/Documents utiles ».***

#Les personnels dont le séjour à l'ICCF serait inférieur à 1 mois et les stagiaires qui ne sont pas en stage à temps plein à l'ICCF n'auront pas de badge.

Annexe n°2
Charte d'Hygiène et Sécurité

L'activité de recherche n'est pas exempte de risques.

LA SECURITE EST L'AFFAIRE DE TOUS

La présente charte a pour objet de faire prendre conscience, à chacun, des risques présents au sein de l'Institut et d'être acteurs de la prévention.

LA PRÉVENTION NE PEUT ÊTRE QU'UNE ACTION COLLECTIVE

Chacun doit se préoccuper de sa propre sécurité et de celle des autres (collègues, agents d'entreprises extérieures, étudiants). Chacun doit s'informer des bonnes pratiques de travail, des dispositions à prendre en cas d'accident ou de sinistre et être conscient des responsabilités engagées.
Dans ce but, les règles de base d'hygiène et sécurité de l'Institut de Chimie de Clermont-Ferrand sont présentées à tous les nouveaux entrants de l'ICCF par l'intermédiaire d'une formation Hygiène et Sécurité. Le document présenté lors de cette formation recense :
- L'organigramme de l'Institut.
- L'organisation et les acteurs H&S de l'ICCF et du campus universitaire.
- Les règles de base de la sécurité en laboratoire.
- Les bonnes pratiques dans un laboratoire de chimie.
- Les risques susceptibles d'être rencontrés au sein de l'Institut.
- La gestion des déchets quelle que soit leur nature.
- La procédure à suivre en cas d'évacuation.
- Les protocoles à suivre pour « l'appel des secours » en cas d'incident ou d'accident.

- Une information sur les horaires et jours d'ouverture du laboratoire et sur la notion de travail isolé.

La présentation de cette charte s'effectue soit en groupe lors de sessions groupées (arrivée des stagiaires de filière de l'université) soit individuellement pour les étudiants ou stagiaires arrivant en décalé. Suite à la présentation, les personnes formées émargent soit sur une feuille de présence lors des sessions groupées soit sur une déclaration individuelle indiquant qu'ils ont suivi la formation.

En signant cette feuille, chacun s'engage à respecter l'ensemble des consignes présentées, mais également à s'informer régulièrement des nouveaux dispositifs mis à leur disposition.
La formation Hygiène et Sécurité adaptée au poste de travail de chaque agent-stagiaire-visiteur se fait par le responsable du poste de travail ou par l'encadrant du stagiaire. Elle peut également être complétée par l'Assistant de Prévention du bâtiment. L'ensemble des informations et équipements nécessaires à la santé et la sécurité des agents est mis à la disposition de ceux-ci.

TRANSPORT DE MATIERES DANGEREUSES

Le transport de marchandises (matières premières, échantillons, produits de synthèse, toute matière issue de l'activité scientifique de l'Institut, matériel scientifique …) constitue une opération où le moindre accident peut entrainer les conséquences les plus graves.

C'est pourquoi ce type de transport fait l'objet d'une réglementation complexe et exigeante (directive n°94/55 du 21 novembre 1994, « directive ADR », arrêté du 5 décembre 1996 applicable jusqu'au 31/12/2002, arrêté du 1er juin 2001 abrogeant l'arrêté de 1996 pour le transport des

matières dangereuses - loi n°75-633 du 15 juillet 1975 et décret n° 98-679 du 30 juillet 1998 pour le transport des déchets par route).

Dans ce cadre, l'Institut fait recours aux services d'ULISSE (ULISSE UPS n°9669), comme demandé dans la circulaire CIR131514DAJ du 10 juillet 2013 de la Présidence du CNRS.
A ce titre, l'Institut dispose d'un Conseiller à la sécurité des TMD (Transport de Matières Dangereuses) : Monsieur Marc Bernier (04 50 11 08 24, marc.bernier@ulisse.cnrs.fr).

Par conséquent, UPS ULISSE est le seul prestataire habilité à assurer l'étude et la réalisation de tous types d'opérations logistiques, nationales, européennes et internationales au sein de l'Institut.
Le non-respect de ces normes et de cette circulaire peut entrainer la mise en cause de la responsabilité pénale des personnes morales et physiques, intervenant dans l'organisation et la réalisation d'un TMD.

Institut de Chimie de Clermont-Ferrand
ICCF - UMR 6296

Attestation

Je soussigné(e) ---------- , certifie avoir pris connaissance du règlement intérieur de l'ICCF, ainsi que de la charte d'Hygiène et Sécurité.

Fait à Aubière, le ----------

Chimie 7 - 24, avenue Blaise Pascal, TSA 60026 CS 60026, 63178 AUBIERE Cedex – France
☎ : (33) 04 73 40 71.25
: direction.iccf@uca.fr https://iccf.uca.fr/

UNIVERSITÉ
Clermont Auvergne

CHARTE GENERALE A L'USAGE DES RESSOURCES NUMERIQUES

Université Clermont Auvergne

Table des matières

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 :

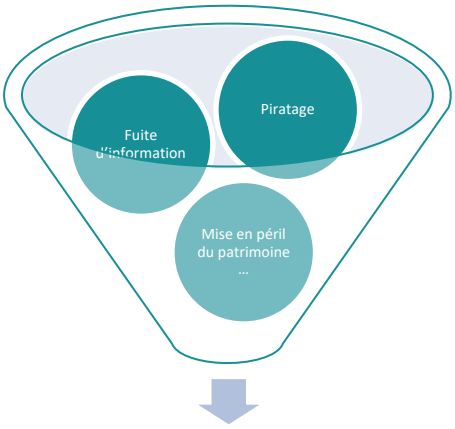
Terme utilisé	Définition	Commentaires
Etablissement	l'Université Clermont Auvergne	Prise en tant que personne morale disposant d'une capacité juridique
Administrateur	Agent ou prestataire chargé par la direction des systèmes d'information de l'Université Clermont Auvergne d'administrer et contrôler l'utilisation 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'approprier 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.



Les risques relatifs aux Ressources numériques sont nombreux

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, ordiphones et sous-jacents : serveurs, switchs, 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.

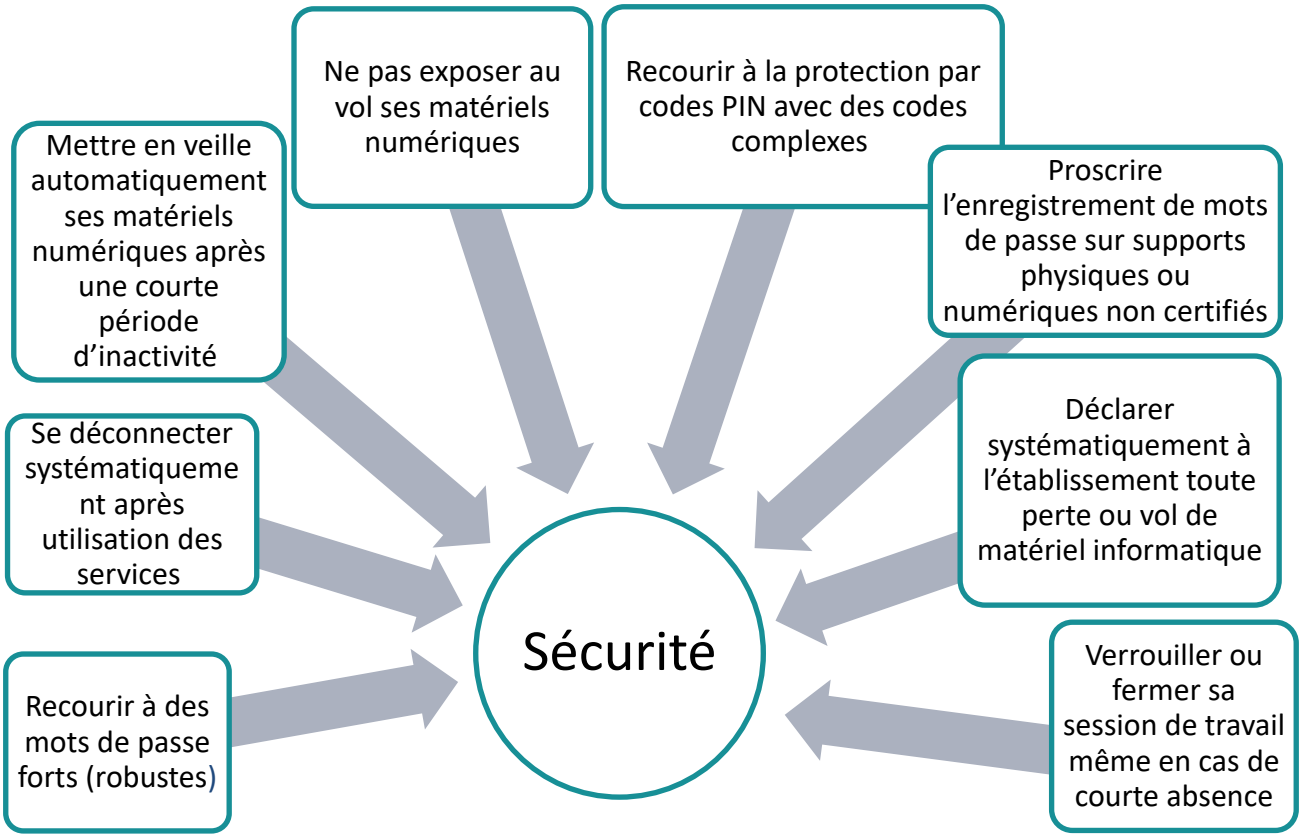
Cette Autorisation est confiée à titre personnel par l'Administrateur à chaque Usager et pour une durée déterminée correspondant le plus souvent à la durée de sa Mission.

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 incessible. 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'Etablissement recommande à ses Usagers les mesures suivantes :



Liste non exhaustive donnée à titre indicatif

A ces fins, l'usager 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'Etablissement.

L'Usager ne peut s'opposer au droit de l'Etablissement 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 boite de messagerie fonctionnelle (par exemple directeur.dsi@uca.fr). Celle-ci sera ainsi consultable par plusieurs personnes en cas de votre abscence et permettra d'assurer plus facilement la continuité de service.

3. Devoir d'information

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

Chaque Usager est tenu d'informer l'Etablissement, 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'Etablissement 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'Etablissement

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

L'Etablissement est soumis à des obligations légales en ce qui concerne l'utilisation de ses Ressources numériques. Notamment, l'Etablissement 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'Etablissement peut être amené à produire ces logs de connexion dans le cadre d'une réquisition judiciaire. En aucun cas l'Etablissement 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 judicaire 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 (DAJI).