Règlement intérieur du Laboratoire de Biométrie et Biologie Evolutive

PREAMBULE

L'Unité Laboratoire de Biométrie et Biologie Evolutive - 5558 (ci-après désignée l'« Unité ») est une UMR placée sous la responsabilité conjointe du CNRS et de l'Université Lyon 1. Elle est implantée dans les locaux de l'Université Lyon 1.

Le présent règlement intérieur a été soumis à l'avis du Conseil de laboratoire, réuni le …

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 Claude Bernard Lyon 1, organisme hébergeant de l'Unité. En cas de contradiction, les dispositions de l'organisme hébergeur prévaudront.

Toute modification sera soumise à l'avis du Conseil de laboratoire 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

Chapitre 1 : Fonctionnement....3
Article 1 : Fonctionnement général de l'Unité....3
Chapitre 2 : Ressources humaines....4
Article 2 : Durée du travail....4
Article 3 : Horaires....5
Article 4 : Congés....5
Article 5 : Télétravail....8
Article 6 : Absences....8
Article 7 : Mission....8
Chapitre 3 : Santé et sécurité....9
Article 8 : Personnes ressources en matière de sécurité et de prévention des risques....9
Article 9 : Organisation de la prévention au sein de l'unité....10
Article 10 : Interdictions....12
Chapitre 4 : Confidentialité, publications et communication, propriété intellectuelle....12
Article 11 : Confidentialité, publications et communication, propriété intellectuelle....12
Chapitre 5 : Dispositions générales....15
Article 12: Discipline....15
Article 13 : Formation....15
Article 14 : Utilisation des moyens informatiques et Sécurité des systèmes d'information....15
Article 15 : Utilisation des ressources techniques collectives....16
Article 16 : Durée....16
Article 17 : Publicité....16
ANNEXE N°2 : RÔLE ET MISSIONS DE L'ASSISTANT DE PREVENTION....22
ANNEXE N°3 : NOTE SUR LE TRAVAIL ISOLE....23
ANNEXE N°4 : CHARTES SUR LA SECURITE DES SYSTEMES D'INFORMATION....26
ANNEXE N°5 : MODALITES DE SAUVEGARDE....50
DES POSTES DE TRAVAIL INFORMATIQUE....50
ANNEXE N°6 : MODALITES D'UTILISATION DES VEHICULES DE SERVICE....51

Chapitre 1 : Fonctionnement

Article 1 : Fonctionnement général de l'Unité

1.1 : Assemblée générale

L'Assemblée Générale comprend tous les personnels de l'Unité. Elle est réunie sur convocation du Directeur d'Unité notamment lors du dernier trimestre de l'année civile pour une présentation générale des services de l'Unité (pôle administratif, pôle informatique, pôle biotechnologique, hygiène et sécurité) à l'attention des nouveaux entrants. A cette occasion, les nouveaux entrants se présentent aux membres de l'Unité (équipe d'accueil, compétences, projet de recherche).

1.2 : Conseil de laboratoire

1-2-1 Composition

En application de la décision n° 920368SOSI du 28 octobre 1992 modifiée relative à la constitution, la composition, la compétence et au fonctionnement des conseils de laboratoire des structures opérationnelles de recherche et des structures opérationnelles de service du CNRS, le Conseil de laboratoire de l'Unité se compose de 20 membres :

- membres de droit : le Directeur d'Unité
- membres nommés : 5
- membres élus : 14

1-2-2 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 des avis formulés par l'HCERES et 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 est associé à la préparation du rapport d'activité.

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.

1-2-3 Fonctionnement

Le Conseil de laboratoire est présidé par le Directeur de l'Unité. Il se réunit au moins trois fois par an. Il est convoqué par mail, un compte-rendu est diffusé à tous les membres de l'unité (mail et intranet du laboratoire).

1.3 Autres : - Comité de Direction – Réunion des chefs d'équipe et responsables ou représentants de pôle

Le comité de Direction :
Il est présidé par le Directeur d'Unité et est constitué des Directeurs des quatre départements scientifiques et de la Responsable administrative de l'Unité. Il traite de toutes les questions relevant de la gestion et du fonctionnement de l'Unité.

La réunion des chefs d'équipe et responsables ou représentants de pôle :
Elle est présidée par le Directeur d'Unité. Elle est un lieu d'échange bidirectionnel d'informations entre les équipes de recherche, les pôles techniques et administratif et la direction de l'Unité. Toutes les questions concernant la politique scientifique et l'organisation de l'Unité peuvent y être abordées.

1.4 Organisation de l'Unité

L'unité est composée de :
- 15 équipes de recherche, structurées en 4 départements. Chaque équipe et département désignent un responsable.
- 4 pôles techniques. Chaque pôle technique désigne un responsable ou un représentant.
- 1 Service hygiène et sécurité composé des agents de prévention de l'unité et du référent expérimentation animale sous la responsabilité du Directeur d'Unité
- 1 service communication composé de la responsable administrative de l'Unité, d'un représentant de chaque département et d'un représentant des formations sous la responsabilité du Directeur d'Unité

1.5 Accès aux systèmes d'information (SI) de l'Unité

Les membres de l'Unité ont accès aux SI de l'Unité à condition d'avoir, au préalable, pris connaissance des Chartes de la Sécurité des Systèmes d'Information placées en annexe. En tout état de cause les personnes non concernées par les activités de l'Unité ne peuvent avoir accès aux systèmes d'information de l'Unité sans l'autorisation du Directeur d'Unité.

1.6 Accès aux locaux

Les accès aux locaux de l'unité se font par badge nominatif

L'accès aux locaux en dehors de la plage horaire de travail de référence est expressément et nommément autorisé par le Directeur de l'Unité.

Les personnes non concernées par les activités de l'Unité ne peuvent avoir accès aux locaux sans l'autorisation du Directeur en dehors des cas prévus par la règlementation relative aux droits syndicaux ou en cas d'urgence.

Toute personne quittant l'Unité (démission, mutation, départ à la retraite, fin de stage, fin de contrat …) doit libérer les locaux et restituer l'ensemble des moyens d'accès à ceux-ci (clé, badge…).

Chapitre 2 : Ressources humaines

Article 2 : Durée du travail

Le personnel nécessaire au fonctionnement de l'Unité est affecté à celle-ci par décision des tutelles qui restent individuellement employeur de leurs agents. Chaque agent affecté à l'Unité est régi, pour ce qui concerne les dispositions relatives à ce chapitre, par les dispositions statutaires propres à son cadre d'emploi et aux règles en vigueur dans l'établissement qui verse sa rémunération.

La durée annuelle de travail est fixée à 1 607 heures en référence au code du travail. Cette durée tient compte des 7 heures de travail dues au titre de la journée de solidarité.

Les dispositions décrites ci-dessous concernent les personnels du CNRS et de l'Université Lyon 1 ; les personnels relevant d'autres organismes suivent les règles qui s'appliquent à eux.

Pour les personnels CNRS : la durée annuelle de travail est fixée à 1 607 heures. Cette durée tient compte des 7 heures de travail dues au titre de la journée de solidarité (les modalités d'accomplissement de cette journée sont précisées à l'article 4.3 du présent règlement intérieur).
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 Université Lyon 1 : le décompte du temps de travail est réalisé sur la base d'une durée annuelle de travail effectif de 1607 heures. Cette obligation annuelle de service ne modifie pas le décompte des jours de travail qui s'effectue toujours sur la base de 1600 heures (les 7 heures supplémentaires correspondent à la journée de solidarité). Son déduits deux jours de fractionnement des congés (sur la base de 7 heures par jour) ce qui ramène l'horaire à 1586 heures

Article 3 : Horaires

Le personnel est tenu au respect des horaires et de la durée du travail fixés en fonction des dispositions statutaires et règlementaires relatives à la durée hebdomadaire de travail et aux congés fixés par son employeur et en tenant compte des nécessités de service de l'Unité.

Les dispositions de la circulaire relative au dispositif concernant l'aménagement du temps de travail ARTT de l'Université Lyon 1 sont applicables.

La durée hebdomadaire du travail effectif pour chaque personnel de l'Unité travaillant à temps plein est fixée sur la base d'un cycle de travail de 5 jours. Elle est calculée en fonction des dispositions réglementaires :
- pour les personnels CNRS, elle est de 38h30
- pour les personnels Université Lyon 1, elle est de 37h30

Pour les personnels CNRS, seuls les personnels autorisés à accomplir un service à temps partiel d'une durée inférieure ou égale à 80 % peuvent travailler selon un cycle hebdomadaire de travail inférieur à 5 jours.
Pour les personnels Université Lyon 1, les personnels à temps complet peuvent effectuer l'intégralité de leurs obligations en 4.5 jours sans incidence sur leurs droits à congé.

Le temps de travail correspond au temps de travail effectif. Il ne prend pas en compte la pause méridienne qui ne peut être :
- ni inférieure à 45 minutes ni supérieure à 2 heures pour les personnels du CNRS,
- ni inférieure à 1 heure ni supérieure à 2 heures pour les personnes de l'Université Lyon 1

Les personnels Université Lyon 1 dont le temps de travail quotidien atteint 6 heures bénéficient d'un temps de pause d'une durée de 20 minutes, non fractionnable, et inclus dans les obligations quotidiennes de service. Cette pause s'effectue toujours à l'intérieur de la journée et non en début ou en fin de journée. Ce temps peut être ajouté au temps de restauration de l'agent.

La plage horaire de travail de référence commence à 7 heures et se termine à 20 heures les jours ouvrés.

Après accord du Directeur de l'Unité et sous réserve des nécessités de service, certains personnels peuvent pratiquer un horaire décalé par rapport à la plage horaire de référence.

Article 4 : Congés

4.1. Congés annuels et RTT

Le nombre de jours de congés annuels et le nombre de jours accordés au titre de l'aménagement du temps de travail sont fixés dans le respect des dispositions statutaires et règlementaires telles que définies par l'employeur de l'agent.

Les dispositions de la circulaire relative au dispositif concernant l'aménagement du temps de travail ARTT de l'Université Lyon 1 sont applicables.

Pour le personnel CNRS :

L'agent travaillant selon une durée hebdomadaire de travail de 38h30 bénéficie de :
- 32 jours ouvrés de congés annuels (du lundi au vendredi) par année civile (du 1er janvier au 31 décembre) ;
- 12 jours au titre de l'Aménagement et de la Réduction du Temps de Travail (jours RTT) ;
- 1 à 2 jours de congés accordés au titre du fractionnement (1 jour quand les congés sont pris entre la période du 31 octobre au 1er mai pour une durée de 5 à 7 jours et 2 jours si cette durée est au moins égal à 8 jours).

Les agents exerçant leurs fonctions à temps partiel bénéficient d'un nombre de jours de congés annuels et de jours RTT calculés en fonction de leurs obligations hebdomadaires de service. Par exemple, un agent travaillant selon une quotité de temps de travail de 80% sur 4 jours bénéficie de 26 jours de congés annuels (32x4/5). En revanche, l'agent travaillant selon une quotité de temps de travail de 80% sur 5 jours bénéficie du même nombre de jours de congés annuels qu'un agent exerçant ses fonctions à temps plein soit 32 jours.

Les jours RTT sont, quant à eux, proratisés en fonction de la quotité de temps de travail de l'agent. Par exemple, le nombre de jours de congés annuels et RTT d'un agent exerçant ses fonctions à temps partiel selon une quotité de temps de travail de 80% sur 4 jours est calculé au prorata de la quotité travaillée. En revanche, l'agent travaillant à temps partiel selon une quotité de temps de travail de 80% sur 5 jours bénéficie du même nombre de jours de congés annuels et RTT qu'un agent exerçant ses fonctions à temps plein.

Les jours de fractionnement auxquels les agents à temps partiel ont droit, le cas échéant, ne sont pas proratisés.

Les jours de fêtes légales, dont la liste est déterminée annuellement par le Ministère chargé de la Fonction Publique comme pouvant être chômés et payés pour l'ensemble des personnels de l'Etat, ne donnent pas lieu à récupération même lorsque ces jours coïncident avec une journée de temps partiel.

Les jours de fermeture de l'Unité sont décidés au début de chaque année par le Directeur de l'Unité après avis du conseil de laboratoire et en fonction des règles en vigueur dans l'établissement hébergeur. Ces jours sont décomptés des jours RTT des agents sauf lorsqu'ils coïncident avec une journée habituellement non travaillée au titre du temps partiel. De la même manière, lorsqu'un jour de fermeture coïncide avec une journée de congé de maladie ou une période de congé tel que congé de maternité, de paternité, d'adoption ou de formation, cette journée décomptée automatiquement en début d'année doit être restituée à l'agent.

Pour les personnels Université Lyon 1

L'agent travaillant selon une durée hebdomadaire de travail de 37h30 bénéficie de :
- 45 jours ouvrés de congés annuels (du lundi au vendredi) par année universitaire (1er septembre au 31 août) plus deux jours de fractionnement, soit 47 jours ouvrés ;
- S'ajoutent 2.5 jours de récupération de travail supplémentaire accompli au-delà du nombre arithmétique quotidien (compensation des 5 minutes : horaire théorique 7h25, horaire réel 7h30) soit 49.5 jours moins la journée de solidarité (sauf lors des années bissextiles où lorsque le 29 février est un jour ouvré, la journée de solidarité est considérée comme correspondant à cette date).
Total : 48.5 jours ouvrés.

A l'exception des congés bonifiés, l'absence du service ne peut excéder 31 jours consécutifs, incluant les week-ends.

Les jours fériés légaux font chaque année l'objet d'un calendrier annuel publié par le Ministère de la Fonction Publique. Ils sont comptabilisés comme du temps de travail effectif, pour le nombre d'heures de travail prévu dans l'emploi du temps de la semaine concernée, lorsqu'ils sont précédés ou suivis d'un jour travaillé, à l'exception des jours fériés survenant un dimanche ou un samedi habituellement non travaillés et de ceux survenant pendant une période de congés des personnels (congés annuels, temps partiel) qui ne sont pas décomptés des congés ni récupérables. Ils se décomptent au fur et à mesure du déroulement du calendrier. Il en résulte que les jours fériés intervenant pendant une période de congés des personnels ne

s'imputent pas sur le nombre de congés annuels mais constituent des jours chômés qui viennent s'ajouter aux jours de congés annuels, sans diminuer pour autant la durée annuelle de travail de référence.

4.2. Conditions d'octroi et d'utilisation

4.2.1 Conditions d'octroi

L'octroi des congés fait nécessairement l'objet d'une demande préalable auprès du Directeur d'Unité via les applications Agate (https://agate.cnrs.fr/) pour le personnel CNRS ou GH2C (https://conges.univ-lyon1.fr) pour le personnel Université Lyon 1 à l'exception des personnels enseignants-chercheurs et assimilés tels que doctorants exerçant une activité complémentaire d'enseignement.

Les congés sont accordés sous réserve des nécessités du service.

4.2.2 Conditions d'utilisation

L'absence de service ne peut excéder 31 jours consécutifs (la durée du congé est calculée du premier au dernier jour sans déduction des samedis, dimanches et jours fériés) [sauf disposition spécifique liée à la fermeture du site].

Pour le CNRS, le report des jours de congés annuels et des jours RTT non utilisés pendant l'année civile est autorisé jusqu'au 28 février de l'année suivante. Les jours qui n'ont pas été utilisés à cette date sont définitivement perdus sauf si ces jours ont été épargnés sur un compte épargne temps.

Pour le personnel Université Lyon 1, le report des jours de congés annuels non utilisés pendant l'année universitaire précédente est autorisé jusqu'au 31 décembre de l'année en cours sous réserve de l'acceptation du supérieur hiérarchique. Les jours qui n'ont pas été utilisés à cette date sont définitivement perdus sauf si ces jours ont été épargnés sur un compte épargne temps.

Le suivi des congés (annuels et RTT) est réalisé dans l'Unité sous la responsabilité du Directeur de l'Unité, à l'aide des applications Agate et GH2C.

4.3 Journée de solidarité

En application de la loi n°2004-626 du 30 juin 2004 modifiée, les agents de l'Unité sont tenus d'effectuer une journée de solidarité de 7 heures accomplie selon la modalité suivante :

Pour le personnel CNRS, cette journée prend obligatoirement la forme d'un jour RTT déduit en début d'année du contingent annuel de jour RTT.

La valeur horaire d'un jour RTT étant supérieure à 7 heures (7h42 pour un agent à temps assujetti à un durée hebdomadaire de 38h30), la différence entre la valeur horaire d'un jour RTT et les 7 heures accomplies au titre de la journée de solidarité est récupérée sous forme de temps de repos (soit un récupération de 42 minutes pour un agent à temps plein assujetti à une durée hebdomadaire de 38h30).

Pour un agent exerçant ses fonctions à temps partiel, le nombre d'heures dû au titre de la journée de solidarité est proratisé en fonction de la quotité de temps de travail et donne lieu à une récupération en temps de repos du temps supplémentaire accompli par rapport à la valeur horaire d'un jour RTT.

4.4. Compte épargne temps (CET)

Tout agent titulaire ou non titulaire de l'Unité, employé de manière continue depuis au moins un an dans une administration de l'Etat, un établissement public à caractère administratif de l'Etat ou un établissement public local d'enseignement, peut ouvrir un CET.

Les conditions d'alimentation et d'utilisation du CET sont fixées par le décret n°2002-634 du 29 avril 2002 modifié et par son arrêté d'application du 20 janvier 2004 modifié.

<u>Pour le personnel CNRS :</u>

Le CET peut être alimenté dans l'application Agate au plus tôt le 1er novembre et au plus tard le 31 décembre de l'année.

La gestion et le suivi du CET sont confiés au service des ressources humaines de la délégation régionale du CNRS.

Pour le personnel Université Lyon 1 :
Le CET peut être alimenté dans l'application GH2C entre le 1er novembre et le 31 décembre de l'année.

Article 5 : Télétravail

Tous les personnels du laboratoire peuvent demander à exercer une partie de leur activité en télétravail conformément au décret n°2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature et à l'arrêté ministériel fixant son application.

Article 6 : Absences

6.1. Absence pour raison médicale

Toute indisponibilité consécutive à la maladie doit, sauf cas de force majeure, dûment être justifiée et signalée au Directeur de l'Unité dans les 24 heures. Sous les 48 heures qui suivent l'arrêt de travail l'agent doit produire un certificat médical.

6.2. Autres autorisations d'absence

Les personnels CNRS et Université Lyon 1 peuvent bénéficier d'autorisations exceptionnelles d'absence non imputées sur les droits à congés annuels/RTT. Hormis quelques autorisations exceptionnelles d'absence dont l'octroi est de droit (par exemple : participation à un jury d'assises, examens médicaux dans le cadre de la grossesse...), la plupart des autorisations d'absence constituent de simples mesures de bienveillance soumise à l'approbation préalable du responsable hiérarchique qui apprécie la demande en fonction de l'exigence liée aux nécessité de service.

Pour en bénéficier il convient de faire une demande auprès de la responsable administrative du laboratoire sur présentation d'un justificatif, notamment pour les motifs suivants :

- Evènements de famille (mariage, pacs, décès ...)
- Fêtes religieuses
- Concours et examens professionnels
- Enfant malade
- Déménagement

Article 7 : Mission

Tout agent se déplaçant pour l'exercice de ses fonctions, doit être en possession d'un ordre de mission délivré préalablement au déroulement de la mission par le Directeur de l'Unité. Ce document assure notamment 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 CNRS ainsi que des enseignants-chercheurs de l'Université dans certains pays étrangers.

L'agent amené à se rendre directement de son domicile sur un lieu de travail occasionnel sans passer par sa résidence administrative habituelle doit nécessairement être en possession d'un ordre de mission.

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.

Chapitre 3 : Santé et sécurité

Article 8 : Personnes ressources en matière de sécurité et de prévention des risques

8.1 Directeur d'Unité

Il lui incombe de veiller à la sécurité et à la protection des agents placés sous son autorité et d'assurer la sauvegarde des biens dont il dispose.

En fonction de la taille de l'Unité et des risques liés aux activités, il nomme, après avis du conseil de laboratoire, un (ou plusieurs) Agent(s) de Prévention (AP), placé(s) sous son autorité qui l'assiste(nt) et le conseille(nt) dans le domaine de la prévention et de la sécurité.

La nomination d'assistant(s) de prévention est sans incidence sur le principe de responsabilité du Directeur d'Unité.

8.2 Assistant de prévention

Le rôle de conseil et d'assistance porte sur la démarche d'évaluation des risques, la mise en place d'une politique de prévention ainsi que sur la mise en œuvre des règles d'hygiène et de sécurité dans l'Unité.
Nom(s) et les coordonnées de(s) assistants de prévention :

- Hélène Henri – 04 72 43 29 14 - helene.henri@univ-lyon1.fr – Risques chimiques et biologiques liés à l'expérimentation de l'Unité sur le site de La Doua (bâtiment Mendel)
- Stéphane Delmotte – 04 72 43 11 68 - stephane.delmotte@univ-lyon1.fr – Risques incendie et risques électriques de l'Unité sur le site de la Doua (bâtiment Mendel)
- Pascale Chevret – 04 72 44 85 61 - pascale.chevret@univ-lyon1.fr - Risques chimiques et biologiques liés à l'expérimentation de l'Unité sur le site de La Doua (bâtiment Mendel)
- Benjamin Rey – 04 72 43 29 29 - benjamin.rey@univ-lyon1.fr – Risques associés aux expérimentations de terrain – Risques biochimiques liés à l'utilisation d'acides, bases, solvants organiques) et d'écophysiologie dans les salles n°15 biochimie 1er étage du bâtiment Mendel et n°20 écophysiologie 2ème étage du bâtiment Mendel)

8.3 Equipiers de sécurité Incendie

Noms, coordonnées et localisation dans l'Unité des chargés d'évacuation (guide-file, serre-file)
- Nelly Burlet – 04 72 43 29 17 – nelly.burlet@univ-lyon1.fr – 1er étage bâtiment Mendel – bureau 153
- Emmanuel Desouhant – 04 72 43 26 33 – emmanuel.desouhant@univ-lyon1.fr – 1er étage bâtiment Mendel – bureau 111
- Benjamin Rey- 04 72 43 29 29 - benjamin.rey@univ-lyon1.fr – 1er étage bâtiment Mendel – bureau 129
- Laurent Jacob – 04 72 44 85 98 – laurent.jacob@univ-lyon1.fr – 1er étage bâtiment Mendel – Bureau 140
- Nathalie Arbasetti – 04 72 44 81 42 – nathalie.arbasetti@univ-lyon1.fr – 1er étage bâtiment Mendel – bureau 139
- Pascale Chevret - 04 72 44 85 61 - pascale.chevret@univ-lyon1.fr – 1er étage bâtiment Mendel – bureau 160
- Laurent Duret – 04 72 44 62 97 – laurent.duret@univ-lyon1.fr – 2ème étage bâtiment Mendel – Bureau 218
- Gabriel Marais - 04 72 43 29 09 – gabriel.marais@univ-lyon1.fr – 2ème étage bâtiment Mendel – Bureau 217
- Stéphane Delmotte - 04 72 43 11 68 - stephane.delmotte@univ-lyon1.fr – 2ème étage bâtiment Mendel – Bureau 206
- Arnaud Mary – 04 72 43 15 52 – arnaud.mary@univ-lyon1.fr – Mezzanine – bureau 8
- Christelle Lopes – 04 72 44 80 51 – chritelle.lopes@univ-lyon1.fr – Mezzanine – bureau 4

8.4 Personnes compétentes dans un domaine de gestion du risque

Noms, coordonnées et localisation dans l'Unité du :
- Responsable de gestion de déchets : Hélène Henri - 04 72 43 29 14 - helene.henri@univ-lyon1.fr
- Correspondant Expérimentation animale : Ludovic Say – 04 72 69 20 66 – ludovic.say@univ-lyon1.fr

8.5 Membres de l'instance de concertation

Le LBBE ne possède pas de commission hygiène, sécurité et condition de travail. Les problématiques relevant de la santé et de la sécurité au travail seront traitées au moins une fois par an au sein du conseil d'Unité. Dans ce cas, l'AP (ou les AP) est (sont) invité(s) à y participer.

Les CHSCT (Comité d'Hygiène, de Sécurité et des Conditions de Travail) des établissements de tutelle sont informés des questions d'hygiène et de sécurité traitées au sein de cette instance. Les membres qui les composent sont indiqués :

- pour le CNRS via le lien suivant https://extranet.dr7.cnrs.fr/alaune/sante-securite-travail/acteurs/chs.html#
- pour l'Université Lyon 1 via le lien suivant http://intranet.univ-lyon1.fr/hygiene-securite/chsct-central/chsct-central-53539.kjsp?RH=1437567877349

Article 9 : Organisation de la prévention au sein de l'unité

9.1 Suivi médical des agents

Les agents bénéficient d'un suivi médical dont la périodicité est définie par le médecin de prévention (tous les 5 ans minimum ou surveillance médicale particulière en fonction de l'exposition à des risques déterminés et / ou de l'état de santé de l'agent).
Noms et les coordonnées des médecins de prévention :
- pour les agents CNRS : Laurette Rocher – 04 72 69 26 89 - Laurette.Rocher@cnrs.fr
- pour les agents Université Lyon 1 : Nicole Barborier – 04 72 44 82 11 - service.medical-DOUA@univ-lyon1.fr

9.2 Mesures de prévention spécifiques en fonction de l'activité et des risques

Les modalités d'accès aux plateaux techniques du laboratoire, leur localisation, leurs responsables sont détaillés dans l'annexe n° 1.
Cette annexe précise aussi les équipements de protection individuelle à utiliser.

9.3 Organisation des secours

Les membres de l'unité sont tenus de prendre connaissance des panneaux d'évacuation situés dans les locaux de l'Université Lyon 1 et devront se soumettre aux exercices d'évacuation organisés par l'Université Lyon 1, tutelle hébergeant l'unité.
En cas d'urgence il convient de composer le 30 ou le numéro externe 04 72 44 79 74.
Ces numéros sont affichés dans les locaux du LBBE.

9.4 Conduite(s) à tenir en cas d'accident lié à une activité spécifique

Des fiches pratiques de sécurité des produits chimiques sont disponibles dans chaque salle expérimentale concernée. Ces fiches sont également disponibles auprès des assistants de prévention. La conduite spécifique à tenir en cas d'incident ou d'accident spécifique à ces produits y est clairement indiquée.

Déversement accidentel de produits chimiques

Protéger les victimes et les personnes avoisinantes, ouvrir les fenêtres, se retirer de la zone et fermer la porte en sortant, alerter les personnes compétentes en fonction de la gravité, pratiquer les premier secours éventuels (douche, rince-œil), et prévenir le PC sécurité (pour l'Université: le 30).

Projection de produits corrosifs

- Sur la peau

En cas de brûlure thermique ou chimique, respecter la règle des trois 15 sans ôter les vêtements: refroidir la plaie pendant 15 minutes avec une eau à environ 15°C et dont la source d'eau est à environ 15 cm de la plaie. Après ces 15 minutes, en cas de brûlure chimique, ne pas tenter de neutraliser le produit, mettre des gants et retirer les vêtements s'ils n'adhèrent pas à la peau.

- Dans les yeux

Laver immédiatement au sérum physiologique ou à l'eau pendant 10 min, en écartant les paupières, tête inclinée et l'œil atteint positionné vers le bas. Ne pas chercher à neutraliser le produit. Ne pas enlever les lentilles cornéennes.

En cas de brûlure étendue, prévenir le 30 voire le SAMU (15) ou les pompiers (18).

Projection d'azote liquide
- Sur la peau
Ne pas frotter, enlever les vêtements au niveau de la zone touchée, dégeler les parties atteintes par un réchauffement modéré et progressif avec de l'eau à température ambiante pendant 15 minutes au minimum, recouvrir avec un linge propre ou stérile et appeler un médecin.
- Dans les yeux
Contacter les secours et laver immédiatement sous un courant d'eau tiède pendant 15 minutes en écartant les paupières, tête inclinée et œil positionné vers le bas.

Blessures
Si possible, laver la plaie à l'eau et au savon.
Blessure souillée de terre: laver à l'eau et au savon et désinfecter avec un antiseptique. Faire vérifier la validité de la vaccination antitétanique par les services médicaux.
Blessure avec risque d'infection: Laisser saigner la plaie en cas de saignement minime, sans appuyer, la nettoyer à l'eau et au savon et la désinfecter avec un antiseptique. Consulter obligatoirement un(e) infirmier(ère) ou un médecin.

9.5 Accident de service
Le Directeur d'Unité doit immédiatement être informé de tout accident de service, de trajet ou de mission d'agent travaillant dans son Unité, afin qu'il puisse en faire la déclaration à l'employeur de la victime de l'accident.

Une analyse permettant de définir les causes de l'accident devra être menée par le Directeur de l'Unité avec l'aide des assistants de prévention.

9.6 Formation à la sécurité
Une assemblée générale est organisée le dernier trimestre de chaque année à l'attention des nouveaux entrants. Chaque nouvel entrant doit remplir un formulaire qui doit être visé par un des deux responsables du pôle biotechnologie en cas d'expérimentations en laboratoire ou de terrain. Une réunion plus spécifique est organisée par les agents de prévention pour aborder les risques liés à ces expérimentations. Les membres du laboratoire amenés à utiliser les ressources informatiques doivent se présenter auprès du responsable du pôle informatique qui les informe des modalités d'utilisation de ces ressources.

9.7 Registres
Un registre santé sécurité au travail est mis à la disposition du personnel afin de consigner toutes les observations et suggestions relatives à la prévention des risques et à l'amélioration des conditions de travail. Il permet également de signaler tout incident ou accident survenu dans l'Unité.
Ce registre est disponible au pôle administratif de l'unité (pièce 139).

Un registre de signalement de danger grave et imminent, ouvert au timbre du CHSCT compétent, est mis à la disposition des agents à la Présidence de l'Université Lyon 1 – Maison de l'Université.

9.8 Accueil de personnes extérieures
- Stagiaires
Le maître de stage doit s'assurer que le pôle administratif de l'unité a en sa possession la convention de stage signée de toutes les parties avant le début du stage. Aucun stagiaire ne sera autorisé à accéder aux locaux ou à partir en mission sans cette convention.

Le maitre de stage est garant du respect du règlement intérieur par le stagiaire ; il lui remettra le formulaire « nouveaux entrants», lui fera compléter et viser par les personnes qui y sont mentionnées.

Pour tout déplacement hors lieu de stage et toute mission « terrain », le stagiaire devra être muni d'un ordre de mission.

- Visiteurs

Pour les scientifiques invités ou de passage, l'hôte membre de l'unité est garant du respect du règlement intérieur par l'invité.

9.9 Travail isolé

Les situations de travail isolé doivent rester exceptionnelles et être gérées de façon à ce qu'aucun agent ne travaille isolément en un point où il ne pourrait être secouru à bref délai en cas d'accident.

Il appartient au Directeur d'Unité de mettre en œuvre une organisation du travail et une surveillance adaptée pour prévenir les situations de travail isolé, et, à défaut, de délivrer des autorisations de travail hors temps ouvrable, assujetties à l'obligation d'être au minimum deux.

Dans le cas où des travaux dangereux doivent nécessairement être exécutés hors des horaires normaux et/ou sur des lieux isolés ou locaux éloignés, il est obligatoire d'être accompagné ou de mettre en œuvre des mesures compensatoires appropriées.
La note CNRS en date du 30 juin 2010 indique la position du CNRS sur le travail isolé et propose des dispositions et des recommandations relatives à cette problématique (voir note en annexe n°2).

Article 10 : Interdictions

10.1 Animaux domestiques

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

10.2 Interdiction de fumer

En application de l'article L.3511-7 du code de la santé publique, il est interdit de fumer sur les lieux de travail.

10.3 Alcool

Il est interdit de pénétrer ou de demeurer dans l'Unité en état d'ébriété.

La consommation de boissons alcoolisées dans les locaux de travail est interdite sauf autorisation exceptionnelle du Directeur de l'Unité.

Le Directeur d'Unité doit retirer de son poste de travail toute personne en état apparent d'ébriété sur un poste dangereux pour sa santé et sa sécurité, ainsi que pour celles des autres personnes placées à proximité.

Il est interdit à toute personne en état d'ébriété de conduire un véhicule, qu'il soit de service ou personnel.

Chapitre 4 : Confidentialité, publications et communication, propriété intellectuelle

Article 11 : Confidentialité, publications et communication, propriété intellectuelle

11.1 Confidentialité

Les travaux de l'Unité constituent par définition des activités confidentielles.
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.

En l'absence de tout autre accord équivalent déjà signé, les personnels non statutaires accueillis dans l'Unité doivent impérativement signer un accord de confidentialité à leur arrivée.

Pour toute présentation et tout échange sur les travaux et résultats de recherche de l'Unité avec des partenaires publics et/ou privés, la signature d'un accord de secret entre les parties concernées est fortement

recommandée. Les structures de valorisation des établissements de tutelle peuvent être utilement contactées à cet effet.

L'obligation de secret ne peut faire obstacle à l'obligation qui incombe aux chercheurs affectés à l'Unité d'établir leur rapport annuel d'activité pour l'organisme dont ils relèvent, cette communication à usage interne ne constituant pas une divulgation au sens des lois sur la propriété industrielle.

Les dispositions du présent article ne peuvent pas non plus faire obstacle à la soutenance d'une thèse ou d'un mémoire par un chercheur, un boursier ou un stagiaire affecté à l'Unité qui pourra se faire le cas échéant à huis clos.

Les règles déterminant la classification du niveau de confidentialité des informations et des systèmes d'information, les règles de marquage des documents et de cartographie des systèmes d'information, ainsi que les règles concernant les mesures de protection applicables à ces informations et systèmes d'informations figurent dans la Charte Sécurité des Systèmes d'Information donnée en annexe.

11.2 Publications et communication

11.2.1 Autorisation préalable du Directeur de l'Unité

Nonobstant les dispositions de l'article 10.1, les personnels de l'Unité peuvent, en accord avec le responsable scientifique du projet et avec les dispositions contractuelles des conventions dans le cadre desquelles ces publications sont réalisées, publier tout ou partie des travaux qu'ils ont effectué au sein de l'Unité.

En outre, toute publication et communication doit respecter la législation en vigueur et notamment concernant :
- les informations nominatives (déclaration à la CNIL),
- la réglementation PPST (Protection du Potentiel Scientifique et Technique) applicable lorsque le sujet de la publication relève d'un secteur protégé,
- les droits d'auteurs sur les textes, images, sons, vidéos...

11.2.2 Formalisme des publications et communication

Les publications des personnels de l'Unité font apparaître le lien avec les organismes de tutelle. L'affiliation correspond aux dispositions de la convention quinquennale en vigueur.

Un exemplaire de toutes les publications (articles, revues, thèses…) dont tout ou partie du travail a été effectué à l'Unité doit être remis dès parution via le formulaire de saisie des publications du LBBE disponible dans l'intranet du laboratoire à la rubrique « outils – Bibliographie ».

Ces publications doivent également comporter les éventuelles mentions requises par l'organisme contribuant à financer les travaux ayant conduit à la publication.

Les personnels de l'Unité sont tenus de respecter les règles de communication du CNRS explicitées dans la Charte de la Communication du CNRS et/ou des autres établissements de tutelle.

11.2.3 Logos et marques

Les personnels ne peuvent en aucun cas utiliser ni faire référence aux dénominations sociales, logos ou aux marques des tutelle(s) à toute autre fin que la communication scientifique, sans autorisation préalable exprès et écrite desdites tutelle(s).

Pour le CNRS, cette demande d'autorisation doit être présentée au chargé de communication de la Délégation régionale dont dépend l'Unité.

112.4 Création de sites web

La création de sites internet, de blogs et autres diffusions sur internet concernant les travaux d'un ou plusieurs personnels de l'Unité doit faire l'objet d'une autorisation du Directeur de l'Unité ainsi que des représentants des tutelles de l'Unité.

La diffusion d'informations sur les travaux de l'Unité est autorisée seulement sur le site internet officiel de l'Unité après accord du Directeur de l'Unité et, le cas échéant, dans le respect des dispositions contractuelles des conventions dans le cadre desquelles ces publications sont réalisées.

Il est rappelé dans l'installation et la gestion d'un serveur www que le Directeur de l'Unité est responsable de l'information délivrée par le serveur de son laboratoire (cf.http://www.urec.cnrs.fr/article408.html).
De manière analogue à une publication traditionnelle, un serveur doit avoir "un Directeur de publication" qui assure la responsabilité de l'information qui est accessible sur le serveur. Cette fonction ne peut être assurée que par le Directeur de l'Unité. Un serveur doit respecter les lois sur la presse et tous les moyens de diffusion plus classiques.

Toute diffusion d'informations sur support soit papier, soit informatique, soit page web émanant des Unités du CNRS doit respecter la charte graphique du CNRS, consultable à l'adresse : http://www.cnrs.fr/compratique/index.htm et la charte graphique des autres tutelles le cas échéant.

11.3 Cahiers de laboratoire

Il est demandé à tous les personnels de recherche de l'Unité de tenir un cahier de laboratoire afin de garantir le suivi et la protection des résultats de leurs travaux.

Le cahier garantit la traçabilité et la transmission des connaissances. C'est également un outil juridique en cas de litige.

Différents modèles sont disponibles via la Délégation Régionale du CNRS ou des services valorisation des autres tutelles.

Les cahiers de laboratoire appartiennent aux tutelles de l'Unité et sont conservés au laboratoire même après le départ d'un personnel (dans certains cas une copie peut être laissée à l'agent).

Ils sont disponibles au pôle administratif.

11.4 Propriété intellectuelle

Les inventions et droits patrimoniaux sur les logiciels obtenus au sein de l'Unité appartiennent aux tutelles de l'Unité en application de l'article L.611-7 et L113-9 du code de la propriété intellectuelle et conformément aux accords passés entre lesdites tutelles.

Dans tous les cas, les tutelles de l'Unité disposent seules du droit de protéger les résultats issus des travaux de l'Unité et notamment du droit de déposer des titres de propriété intellectuelle correspondants.

Le personnel de l'Unité doit prêter son entier concours aux procédures de protection des résultats issus des travaux auxquels il a participé, et notamment au dépôt éventuel d'une demande de brevet, au maintien en vigueur d'un brevet et à sa défense, tant en France qu'à l'étranger.
Les tutelles s'engagent à ce que le nom des inventeurs soit mentionné dans les demandes de brevets à moins que ceux-ci ne s'y opposent.

Toute personne accueillie au sein de l'Unité, sans lien statutaire ou contractuel avec les tutelles de l'Unité, doit avoir signé à la date de son arrivée dans le laboratoire, une convention d'accueil prévoyant notamment les dispositions de confidentialité, de publications et de propriété intellectuelle applicables aux résultats qu'elle pourrait obtenir ou pourrait contribuer à obtenir pendant son séjour au sein de l'Unité.

11.5 Obligation d'informations du Directeur d'Unité : Contrats, décisions de subvention et ressources propres

Le personnel doit informer le Directeur de l'Unité de tout projet de collaboration, en particulier internationale car elles nécessitent avant signature l'autorisation formelle du ministère de tutelle, et de toute demande de subvention de l'Unité avec des partenaires publics et/ou privés.

Un exemplaire de tout contrat doit être remis au Directeur de l'Unité après sa signature.

Tout achat d'équipement et tout recrutement de personnel doit faire l'objet d'une demande officielle auprès du Directeur de l'Unité.

Chapitre 5 : Dispositions générales

Article 12 : Discipline

Tout manquement aux droits et obligations des agents publics peut faire l'objet d'une sanction disciplinaire.

Pour les personnels CNRS, cette sanction est notifiée par le Délégué régional pour les sanctions du premier groupe (avertissement, blâme) et par le Président du CNRS pour tous les autres groupes de sanctions.

Pour les personnels de l'Université Lyon 1, les sanctions disciplinaires sont prises en application des règles régissant chaque corps de personnels.

Article 13 : Formation

13.1 Correspondant formation

Le correspondant de formation de l'Unité contribue auprès du Directeur de l'Unité au recueil et à l'analyse des besoins de formation et à la définition des objectifs.

Il prépare les différentes étapes de la conception du plan de formation de l'entité, de son déroulement et de son évaluation, en liaison avec le conseiller RH/formation chargé au sein de la Délégation régional du CNRS du suivi des agents.

Le plan de formation est transmis au service des ressources humaines de la Délégation régionale du CNRS.

Le correspondant de formation informe les personnels des actions de formation susceptibles de les intéresser, les assiste et les conseille dans leurs démarches en lien avec le responsable hiérarchique de chaque agent.

13.2 Formation par la recherche

L'encadrement des stagiaires par un agent titulaire ou non de l'Unité est soumis à l'autorisation préalable du chef 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.

Article 14 : Utilisation des moyens informatiques et Sécurité des systèmes d'information

L'utilisation des moyens informatiques de l'Unité est soumise aux dispositions des chartes Sécurité des Systèmes d'Information en vigueur dans l'Unité (Chartes SSI du CNRS, de l'Université Lyon 1 et de Renater).

Ces Chartes ont notamment pour objet de préciser la responsabilité des utilisateurs au regard de la législation. Tout nouvel arrivant utilisateur des moyens informatiques de l'Unité doit déclarer à son arrivée avoir pris connaissance de ces chartes.

Les Chartes Sécurité des Systèmes d'Information figurent en annexe du présent règlement intérieur.

Le CSSI (chargé de la sécurité des systèmes d'information, Bruno Spataro, ingénieur CNRS) assiste et conseille le Directeur d'Unité pour sa politique de sécurité informatique. 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 SI qui concernent le personnel et les systèmes d'information de l'Unité.

Les modalités relatives à la sauvegarde des postes de travail sont décrites en annexe 4.

Article 15 : Utilisation des ressources techniques collectives

- Plateaux techniques. Ce sont :
    Plateforme de Biologie Moléculaire
    Plateforme de Biochimie
    Plateforme d'Eco-physiologie
    Plateforme de Microscopie

Tous les entrants au LBBE quel que soit leur statut doivent venir se présenter à l'un des responsables du pôle biotechnologie, Nelly Burlet ou Benjamin Rey.
L'annexe n° 1 précise les modalités d'utilisation des plateaux techniques.

- Véhicules de service : l'unité dispose de 6 véhicules de service

La gestion du parc automobile est assurée par François Débias, technicien CNRS et Odile Mulet-Marquis, adjointe administrative Université Lyon 1. Ils vérifient le bon état des véhicules et l'entretien régulier aux garages.

Les modalités d'utilisation sont définies en annexe n° 6.

Article 16 : Durée

Le règlement intérieur entre en vigueur à la date de signature par le Délégué régional du CNRS et des représentants dûment habilités des autres tutelles. Il peut être modifié lors du changement de Directeur de l'Unité, à son initiative ou à la demande des tutelles suite à une évolution réglementaire importante et toujours dans le respect des consultations requises au niveau réglementaire.

Dans tous les cas, à la nomination d'un nouveau Directeur de l'Unité, le présent règlement intérieur et ses annexes lui sont remis par le Délégué Régional du CNRS.

Article 17 : Publicité

Le présent règlement intérieur est porté à la connaissance des agents par voie d'affichage dans les locaux de l'Unité et est disponible dans l'intranet du laboratoire.

Il annule et remplace le règlement intérieur du 16 novembre 2012 et entre en vigueur au 1er janvier 2016

Fait à Villeurbanne, le 25 mars 2016

Visa du Directeur de l'Unité **Signature des représentants légaux des tutelles**

ANNEXE N°1 : UTILISATION DES PLATEAUX TECHNIQUES DU LABORATOIRE

Co-responsables du pôle biotechnologique :

Benjamin Rey (IE CNRS) : expérimentations de terrain
Nelly Burlet (AI CNRS) : expérimentations de laboratoire

Liste des plateaux techniques internes à l'unité (2016) et principaux gestionnaires.

Plateforme de Biologie Moléculaire : Hélène Henri ; Nelly Burlet ; David Lepetit
Plateforme de Biochimie : Hélène Henri; Pascale Chevret
Plateforme d'Eco-physiologie : Benjamin Rey; Corinne Régis
Plateforme de Microscopie : Nelly Burlet ; Benjamin Loppin

Agents de prévention pour l'expérimentation

Expérimentation au laboratoire : Hélène Henri (AI CNRS) ;Pascale Chevret (CR CNRS)
Expérimentations de terrain : Benjamin Rey (IE CNRS)
Expérimentation animale : Ludovic Say (PU UCBL)

Accès aux salles et équipements

Les nouveaux entrants (étudiants, stagiaires, chercheurs) désirant mener des expérimentations dans le cadre d'un projet de recherche mené au laboratoire sont tenus de se présenter à l'un des représentants du Pôle Biotechnologique : Benjamin Rey pour les expérimentations de terrain et/ou Nelly Burlet pour les expérimentations de laboratoire.
Cette rencontre a pour objectifs i) d'appréhender la faisabilité au laboratoire ou sur le terrain des expérimentations, ii) d'évaluer les besoins matériels (équipements, consommables) afin de faciliter la gestion de l'utilisation des plateaux techniques, iii) d'identifier les risques (chimiques, biologiques, …) associés aux expérimentations, et iv) de présenter les équipements de protection collectifs et/ou individuels disponibles au laboratoire.
Chaque nouvel entrant sera orienté vers un assistant de prévention. Il sera également inscrit sur la liste mail manip.lbbe@listes.univ-lyon1.fr et s'engagera à participer aux tâches communes pour les expérimentateurs au laboratoire. Les encadrants scientifiques et/ou techniques doivent être identifiés et peuvent participer à cette rencontre.
La fiche « nouvel entrant » signée doit être remise au pôle administratif. Cette démarche est indispensable pour avoir accès aux plateaux techniques.

Règles générales de sécurité liées aux expérimentations

Le port de la blouse est obligatoire dans toutes les salles expérimentales du laboratoire. Les équipements de protection individuelle (gants, masques, lunettes) sont mis à disposition de tous les expérimentateurs qui sont tenus de les utiliser en cas de besoin.
Chaque salle expérimentale dispose de flacons de sérum de rinçage oculaire situés près des éviers.
Les déchets chimiques doivent être conditionnés dans des contenants appropriés et étiquetés selon la réglementation en vigueur en indiquant notamment la nature du produit, sa concentration, et la personne (ou équipe) qui a produit ce déchet. Les assistants de prévention du laboratoire fournissent les contenants vides et se chargent de leur évacuation selon la procédure mise en place par l'Université.

Avant tout montage ou manipulation, il convient de s'informer de l'occupation éventuelle des postes de travail et des opérations qui y sont conduites. Tout poste de travail sur lequel se développent plusieurs manipulations indépendantes constitue une situation potentiellement dangereuse.
Remettre les lieux en l'état d'origine après la manipulation (rangement des appareils, évacuation des produits, étiquetage, nettoyage du poste de travail...), et ceci quel que soit le temps consacré à l'expérience.
Il est interdit de stocker ou absorber de la nourriture ou des boissons dans toutes les zones dédiées aux expérimentations.

Concernant l'expérimentation animale, seules les manipulations avec des animaux couvertes par l'agrément du laboratoire et étant dûment autorisées par le Ministère de l'Enseignement Supérieur et de la Recherche peuvent être mises en œuvre conformément au décret n° 2013-118 du 1er février 2013

- **Plateforme de Biologie Moléculaire**

* Pièce d'extraction ADN en plaque et clonage bactérien (n°1)
Cette pièce comporte 3 postes de travail distincts :

- une hotte chimique permettant l'utilisation de solvants dédiés à l'extraction des acides nucléiques,
- une paillasse dédiée à la réalisation du clonage bactérien. Une étuve et un agitateur de cultures liquides sont mis à disposition dans cette pièce,
- une paillasse dédiée à l'extraction d'acides nucléiques en plaque par l'utilisation d'une pompe à vide. Une centrifugeuse, des pipettes mono et multi-canaux et l'appareil de broyage « tissu lyser » sont dédiés à cette activité.

* Pièce Biologie Moléculaire (n°28)
Cette pièce accueille les activités de biologie moléculaire et comprend:

- des paillasses sur les îlots centraux pour les activités individuelles.
- des paillasses latérales qui hébergent les appareillages à usage collectif (deux hottes dédiées à la préparation des PCR),
- un réfrigérateur et deux congélateurs organisés en tiroirs nominatifs (individuels ou collectifs) permettant le stockage d'échantillons biologiques et/ou réactifs,
- un espace réservé à la manipulation d'ARN

* Pièce électrophorèse (n °29)
Cette pièce est entièrement dédiée à la réalisation d'électrophorèse en gel d'agarose.

Des informations sur le matériel disponible ainsi que sur les procédures à suivre pour les PCR et les électrophorèses sont données à la fin de ce règlement.

- **Plateforme de Biochimie** (Pièce n°15)

Cette pièce peut accueillir les activités suivantes:

- extraction et électrophorèses de protéines,
- stockage de produits chimiques en armoire anti-feu, anticorrosion,
- électrophorèse en acrylamide,
- dosage de biochimie divers.

Cette pièce est équipée de 2 hottes chimiques permettant la manipulation d'acides, de bases, de solvants et de produits chimiques.
Sous chacune de ces hottes la liste des produits autorisés à la manipulation est affichée.
Les produits chimiques dangereux sont stockés dans les armoires chimiques appropriées équipées de système de ventilation, de filtres, disposant d'une fermeture à clés et d'une autonomie de résistance en cas de feu.

- **Plateforme d'éco-physiologie** (Pièce n°20, 2ème étage

Cette pièce offre des possibilités très diverses.
Elle comprend entre autre :

- une paillasse destinée aux prélèvements/dissections de précision sous loupe binoculaire couplée à une caméra et à un ordinateur,
- des paillasses latérales équipées d'appareils à usage collectif (bain marie, balance de précision, étuve, vortex, centrifugeuse, laveur de microplaques…),
- un lecteur de plaques destiné au dosage de composés divers par spectrophotométrie (eg. hormones, protéines, lipides, marqueurs de stress oxydant,…) ainsi qu'à la mesure d'activités biologiques (eg. activités enzymatiques)
- un Poste de Sécurité Microbiologique (PSM) dédié à la manipulation de micro-organismes non pathogènes. **Attention ce PSM ne permet pas la manipulation de solvants organiques ou d'acides**.
- deux réfrigérateurs et trois congélateurs organisés en tiroirs nominatifs (individuels ou collectifs) permettant le stockage d'échantillons biologiques et/ou réactifs,

- des appareils permettant le dosage des acides nucléiques (ADN ou ARN) et des protéines comme le nanodrop, le qubit.

Du matériel commun dédié aux expérimentations sur le terrain est également disponible, la liste est donnée à la fin de ce règlement.

- **Plateforme de microscopie** (Pièce n°27)

Cette salle est accessible uniquement après formation par les responsables.
Cette pièce est équipé d'un microscope numérique à fluorescence (resp : N. Burlet) et d'un microscope confocal (resp : N. Burlet et B. Loppin).
Tout nouveau projet doit être présenté à l'un des responsables de la plateforme afin d'étudier la faisabilité du projet et le matériel nécessaire à sa réalisation.
Chaque utilisateur recevra une **formation adaptée** à ses besoins et **spécifique au microscope** qui sera utilisé.

Chaque utilisateur doit respecter le planning de réservation et est tenu de tenir à jour le cahier de suivi (horaires d'utilisation, filtres utilisés, problèmes).
Tout dysfonctionnement doit immédiatement être rapporté aux responsables de la plateforme. Toute tentative « d'**auto-réparation** » par un utilisateur est formellement **interdite**.

L'utilisation du microscope confocal nécessite la climatisation de la pièce.

Les microscopes numériques à fluorescence et confocal permettent une multitude d'analyses (comptage d'évènements, analyse de colocalisation, expression,…).

Utilisation de l'autoclave
Les personnels formés et habilités à l'utilisation de l'autoclave du LBBE sont :
- Nelly Burlet (AI CNRS)
- François Debias (TCH CNRS)
- Hélène Henri (AI CNRS)
- Nicole Lara (AJT UCBL)
- Sonia Martinez (TCH UCBL)
- Patricia Morales (TCH CNRS)

Chambre climatique Ecoressources
L'accès à cette chambre climatique est restreint au personnel identifié dans le tableau ci-dessous

Programmes	Responsables projet	Responsables technique
Petits rongeurs	Chevret Pascale	Pardonnet Sylvia
Marmottes	Cohas Aurélie	Sauzet Sandrine
Venturia	Desouhant Emmanuel	Gallot Aurore
Carnivores	Devillard Sébastien	Pardonnet Sylvia
Drosophile	Gibert Patricia	Mialdea Gladys
Cervidés	Gilot Fromont Emmanuelle	Debias François
Chats	Pontier Dominique	Régis Corinne
Elephas	Rajon Etienne	Sauzet Sandrine
Curculio	Venner Marie-Claude	Debias François
Treep	Vieira Cristina	Burlet Nelly
Chauve-souris	Pontier Dominique	Régis Corinne

Chaque nouveau projet doit être soumis aux co-responsables de la chambre climatique Ecoressources soit Dominique Allainé et François Débias afin qu'un espace de stockage soit donné et afin de s'assurer que le conditionnement des échantillons est conforme à la politique de gestion de cet espace (identification des échantillons, couleur des boites de stockage,…).

Climatisation dans les salles d'expérimentation
La gestion des climatisations des pièces d'expérimentation et des pièces de stockage est assurée par Gladys Mialdea et Sonia Martinez.

Magasin
Une partie du consommable utilisé couramment est stockée dans un « magasin » et les articles référencés sont à la disposition des expérimentateurs (sous réserve des stocks disponibles). Les co-responsables de la gestion du magasin sont Sonia Martinez et Sandrine Sauzet.
Les demandes d'intégration de nouveaux articles ainsi que la consommation de quantité inhabituelle d'un consommable doivent leur être signalées afin de faciliter la gestion des stocks.

Le magasin est accessible de 9h à 13h du lundi au vendredi en contactant une personne habilitée dans la liste ci-dessous :

- Nelly Burlet (AI CNRS)
- François Debias (TCH CNRS)
- Hélène Henri (AI CNRS)
- Sonia Martinez (TCH UCBL)
- Corinne Régis (TCH UCBL)
- Sandrine Sauzet (TCH CNRS)

En dehors de ces horaires, toute demande de matériel doit se faire via l'adresse mail : magasin.lbbe@univ-lyon1.fr.

Réactifs -20°C
Un congélateur -20°C contient un stockage de réactifs pour la biologie moléculaire fournis par la société Thermoscientific qui assure la gestion. Au même titre que les articles stockés dans le magasin, les réactifs stockés dans ce -20°C sont à la disposition des expérimentateurs. Seules Nelly Burlet, Corinne Régis et Hélène Henri sont habilitées à la sortie des réactifs.

Contribution aux tâches collectives
Chaque expérimentateur est tenu de participer aux tâches collectives.
Le planning est établi chaque trimestre et reste valable jusqu'à l'établissement du nouveau planning. Le planning est transmis par mail via l'adresse manip.lbbe@listes.univ-lyon1.fr et est affiché dans les pièces techniques.

Liste des matériels disponibles et recommandations

- Pièce d'extraction ADN en plaque et clonage bactérien (n°1) :

Centrifugeuses
Pipettes monocanal
Speed Vac
Pompe à vide
Système d'extraction d'acides nucléiques en plaque
Incubateur et agitateur thermostaté dédié au clonage bactérien
Balances de précision

- Plateforme de Biochimie (Pièce n°15) :

Centrifugeuse
Pipettes monocanal
Tissu Lyser (broyeur à billes)
Bain marie
Balances de précision

- Plateforme d'éco-physiologie (Pièce n°20, 2ème étage) :

Centrifugeuse
Pipettes monocanal
Laveur de plaques
Spectrophotomètres
Incubateur

- * Pièce Biologie Moléculaire (n°28) :

Centrifugeuses
Pipettes monocanal, multicanaux et distributrices
Thermomixer
Bain marie
Machine à glace
Speed Vac
Incubateur

- * Pièce électrophorèse (n °29) :

Pipettes mononocanal et multicanaux
Cabine de visualisation des gels avec table UV et caméra reliée à un ordinateur
Cuves à électrophorèse
Générateur
Balance

Mention spéciale sur l'organisation d'une PCR.
Une attention particulière sera portée sur la séparation physique des différentes étapes de la PCR:
- les extractions se font **hors** de la salle 28.
- la préparation des **mix** (les réactifs **sans l'ADN**) se fait sous la **hotte** dédiée (celle de droite),
- l'ajout de l'ADN se fait sur une des paillasses des ilots centraux ou sous la **hotte** dédiée (celle de gauche),
- l'amplification a lieu dans les thermocycleurs de la salle (sans numéro, entre la 12 et la 13),
- le stockage des produits PCR avant migration se fait dans le frigo de la salle d'électrophorèse (n°29),
- la migration a lieu dans la salle électrophorèse (n°29).

Mention spéciale sur le déroulement d'une électrophorèse.
Le tampon d'électrophorèse qui remplit la cuve peut être utilisé jusqu'à 5 fois sans perte de conduction. Pour faciliter l'usage optimal de ce tampon il y a près de chaque cuve un post-it récapitulant le nombre de migrations. Après quoi il peut être évacué dans les bidons dédiés.
La cuve doit être vidée et rincée chaque fin de journée (au minimum) afin d'éviter la cristallisation qui apparaît sur les électrodes lorsque le tampon y stagne trop longtemps et qui réduit considérablement leur durée de vie. Une bouteille de récupération du tampon est prévue près de chaque cuve pour le tampon encore utilisable.

- Matériel commun mis à disposition pour les expérimentations de terrain

Le matériel listé ci-dessous est destiné à faciliter la mise en place de protocoles sur le terrain. Veuillez-vous adresser à Benjamin Rey, François Débias ou Sylvia Pardonnet en cas de besoin.

- GPS à main (Garmin eTrex 20)
- Radio VHF numérique longue portée (Kenwood TK3401D)
- Congélateur -80°C portatif (peut être alimenté sur secteur et sur allume cigare)
- Centrifugeuse portative (alimentation secteur)
- Echographe portatif
- Automate d'hématologie portatif (alimentation secteur)
- Drone quadrimoteur équipé pour la prise de vue aérienne

Des trousses de premier secours sont également disponibles (s'adresser à Sonia Martinez).

ANNEXE N°2 : RÔLE ET MISSIONS DE L'ASSISTANT DE PREVENTION

Le rôle de l'AP est défini dans l'instruction générale n° 122942DAJ relative à la santé et à la sécurité au travail au CNRS

L'agent proposé pour exercer les missions d'AP doit être motivé par les questions touchant à la sécurité et être prêt à recevoir les formations nécessaires. Sa compétence et sa position doivent être reconnues par l'ensemble des personnels de la structure opérationnelle.
L'AP figure à l'organigramme fonctionnel de l'Unité.

Il assure une mission de conseil et d'assistance dans la mise en œuvre des mesures de sécurité et de prévention, ainsi que dans le domaine de la santé au travail.

Il vérifie sous la responsabilité du directeur, que les obligations réglementaires sont bien appliquées dans la structure opérationnelle (aussi bien en matière de fonctionnement que d'infrastructure).

Il propose des mesures préventives de toute nature au Directeur et, après accord de celui-ci, s'assure de la mise en application notamment de celles préconisées par les IRPS, les membres des corps d'inspection et les médecins de prévention.

Il participe aux travaux du comité local d'hygiène et de sécurité et des conditions de travail de la structure opérationnelle. En absence de CLHSCT, il participe au moins annuellement à une séance du conseil représentatif des personnels affectés à la structure durant laquelle les questions de santé et de sécurité au travail sont abordées (conseil de laboratoire, assemblée générale …).

Il sensibilise les agents de la structure opérationnelle au respect des consignes et règles de sécurité et participe à leur formation.

Il informe les nouveaux arrivants dans la structure opérationnelle des dispositions du règlement intérieur, des risques particuliers rencontrés dans la structure opérationnelle et des bonnes pratiques pour les prévenir et participe à leur formation.

Il anime le groupe de travail chargé de l'évaluation des risques professionnels.
Il veille à la mise en place des premiers secours en cas d'accident, et d'une équipe de première intervention spécialisée en cas de risques spécifiques.

Il participe aux visites des installations effectuées par les membres des structures de contrôle et de conseil.

Il tire tous les enseignements des accidents et incidents survenus dans la structure opérationnelle et les communique aux IRPS et aux médecins de prévention.

Il veille à la bonne tenue du registre de santé et de sécurité au travail.

Dans le cas où plusieurs AP sont nommés au sein d'une même structure ou lorsque des personnes compétentes pour des risques spécifiques sont présentes, leurs missions respectives doivent être clairement définies par le Directeur de la structure opérationnelle.

Un entretien visant à établir le bilan de l'activité de l'AP au regard de sa lettre de cadrage est assuré au moins annuellement par le Directeur de la structure opérationnelle, à son initiative.

ANNEXE N°3 : NOTE SUR LE TRAVAIL ISOLE

Paris, le 30 juin 2010

Le Directeur général
Délégué aux ressources

Coordination nationale de prévention et de sécurité
www.cnrs.fr
1 Place Aristide Briand
92190 Meudon
T. 01 47 05 55 05
F. 01 47 05 53 03

Note à l'attention de
Mesdames et Messieurs les directeurs d'instituts et délégués régionaux

Objet : Travail isolé

La question du travail isolé est abordée de façon récurrente dans notre établissement aussi bien au sein des divers comités d'hygiène et de sécurité (national, régionaux, locaux) que lors de réunions spécifiques à la prévention des risques professionnels (IRPS, ACMO, ...).

Cette problématique couvre en réalité des situations très différentes et il convient de les distinguer en deux catégories :
- celles où un travailleur est isolé du fait de son poste de travail
- celles où un travailleur est présent sur son lieu de travail en dehors des horaires d'ouverture.

La première concerne des agents dont une partie de l'activité peut se dérouler dans des locaux géographiquement isolés ou dans lesquels ils sont seuls à travailler (atelier de mécanique, locaux confinés de type animalerie, pièce de culture, locaux de stockage, chambre froide...). Pour ces situations, lorsque les procédures ou organisations internes ne peuvent les éliminer totalement, il conviendra de mettre en œuvre des mesures compensatoires permettant de porter secours rapidement à l'agent en cas d'accident ou de malaise, parmi lesquelles se trouve l'utilisation de dispositifs d'alarme pour travailleurs isolés (DATI, voir annexe).

La seconde catégorie concerne des personnels qui viennent travailler en horaires décalés pour des raisons diverses (expérience en cours, contrainte de temps...).

Ces situations de travail isolé hors temps ouvrable ne sont pas permises et y contrevenir engage la responsabilité des directeurs d'unité.

Il appartient aux Directeurs d'unités de mettre en oeuvre une organisation du travail et une surveillance adaptée pour les prévenir et, à défaut, de délivrer des autorisations de travail hors temps ouvrable (les horaires de travail doivent clairement apparaître dans le règlement intérieur) assujetties à l'obligation d'être au minimum deux.

Cependant, dans les cas où la situation de travail isolé hors temps ouvrable correspond à une **opération ponctuelle d'une durée inférieure à 1 heure** (nourrissage d'animaux par exemple, ...) et **hors zone à risque** (L2, L3, ZS, ZC, ...), le recours à un DATI peut également être envisagé exceptionnellement, après avis de l'IRPS et du CHS compétent .

En conséquence, je souhaite qu'une réflexion soit organisée sur ce sujet dans les unités de recherche pour mettre en œuvre ces dispositions Pour cela, les délégués régionaux voudront bien adresser copie de cette note aux directeurs d'unités de leur délégation.

Des éléments réglementaires ainsi que des propositions de mesures organisationnelles sont présentés dans l'annexe jointe.

Xavier INGLEBERT

Annexe à la note sur le travail isolé

La situation de travailleur isolé

Il s'agit d'une situation où un travailleur est hors de vue ou de portée de voix d'autres personnes et sans possibilité de recours extérieur, aggravée si le travail présente un caractère dangereux.

Si un salarié est physiquement isolé mais que l'organisation ou le contenu de son activité lui permet de communiquer régulièrement avec d'autres personnes à même d'intervenir rapidement en cas d'urgence, il n'est pas considéré en situation de travailleur isolé.

Les textes réglementaires

Il n'existe aucun texte de portée générale sur ce sujet et l'approche réglementaire s'organise donc autour :

- des textes concernant les principes généraux de prévention (Article L4121-1 du code du travail) : *« L'employeur prend les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des travailleurs»*,

- de la réglementation concernant l'intervention d'entreprises extérieures, sur la nécessité d'une alerte, dans le cas du risque lié à l'isolement (art. R4512-13),
  «... le chef de l'entreprise extérieure intéressé prend les mesures nécessaires pour qu'aucun travailleur ne travaille isolément en un point où il ne pourrait être secouru à bref délai en cas d'accident »,

- de différents textes relatifs à un certain nombre de travaux dangereux interdits aux travailleurs isolés et pour lesquels la présence d'un surveillant est requise (ascenseurs, installations électriques, travaux avec rayonnements ionisants...)

Toutefois, le Comité central de coordination (CNAM), dans sa séance du 4 juillet 1966, a émis le vœu suivant : *« Il est recommandé aux directions des entreprises de ne pas faire travailler un salarié seul à un poste de travail dangereux ou essentiel à la sécurité des autres travailleurs. D'autre part, tout salarié ou équipe de salariés dont le poste de travail est isolé du reste de l'entreprise doit faire l'objet d'une surveillance directe ou indirecte de jour comme de nuit ».*

De plus, des recommandations de la CNAM, particulières à certaines branches d'activité professionnelle ont été émises via leurs comités techniques nationaux (recommandations R 252 et R 416).

ANNEXE N°4 : CHARTES SUR LA SECURITE DES SYSTEMES D'INFORMATION

Charte de la Sécurité des Systèmes d'Information du CNRS

Cette charte, annexée au règlement intérieur des Entités, a pour objet d'informer les Utilisateurs de leurs droits et de leurs responsabilités à l'occasion de l'usage des ressources informatiques et des services internet du CNRS, en application de la Politique générale de sécurité de l'information (PGSI) du CNRS et de la législation.

La PGSI en vigueur dans les unités mixtes dépend de l'établissement qui a en charge la politique de sécurité de l'Entité, elle est décidée par accord conventionnel entre les établissements.

Elle répond à la préoccupation du CNRS de protéger les informations qui constituent son patrimoine immatériel contre toute altération, volontaire ou accidentelle, de leur confidentialité, intégrité ou disponibilité. Tout manquement aux règles qui régissent la sécurité des systèmes d'information est en effet susceptible d'avoir des impacts importants (humains, financiers, juridiques, environnementaux, atteinte au fonctionnement de l'organisme ou au potentiel scientifique et technique).

L'Utilisateur contribue à son niveau à la sécurité des systèmes d'Information. À ce titre, il applique les règles de sécurité en vigueur dans l'Entité et signale tout dysfonctionnement ou événement lui apparaissant anormal.

L'Entité met à la disposition de l'Utilisateur les moyens nécessaires à l'application de la politique de sécurité des systèmes d'information.

A son niveau, le personnel d'encadrement favorise l'instauration d'une « culture sécurité » par son exemplarité dans le respect de cette charte et par un soutien actif des équipes en charge de la mise en œuvre de ces règles.

Définitions

On désignera sous le terme « *Utilisateur* » : la personne ayant accès ou utilisant les ressources informatiques et services Internet quel que soit son statut.

On désignera sous le terme « *Entité* » : toutes les entités créées par le CNRS pour l'accomplissement de ses missions, notamment telles que les unités de recherche ou de service propres ou mixtes ainsi que les services et directions administratives.

I. Principes de sécurité

Les règles ci-après s'appliquent à tous les Utilisateurs, et peuvent être complétées par des mesures spécifiques à leur Entité résultant de la PSSI opérationnelle.

Protection des informations et des documents électroniques

Tout Utilisateur est responsable de l'usage des ressources informatiques auxquelles il a accès.

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

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

Lorsque ses données ne font pas l'objet de sauvegardes automatiques mises en place par l'Entité dont il relève, l'Utilisateur met en œuvre le système de sauvegarde manuel préconisé par son Entité.

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

Protection des moyens et droits d'accès aux informations

L'Utilisateur est responsable de l'utilisation des systèmes d'information réalisée avec ses droits d'accès.

A ce titre, il assure la protection des moyens d'authentification qui lui ont été affectés ou qu'il a généré (badges, mots de passe, clés privées, clés privées liées aux certificats, etc.) :

- Il ne les communique jamais, y compris à son responsable hiérarchique et à l'équipe chargée des SI de son Entité ;
- il applique les règles de « génération/complexité » et de renouvellement en vigueur selon le moyen d'authentification utilisé ;
- Il met en place tous les moyens mis à sa disposition pour éviter la divulgation de ses moyens d'authentification ;
- Il modifie ou demande le renouvellement de ses moyens d'authentification dès lors qu'il en suspecte la divulgation.
- Il garantit l'accès à ses données professionnelles, notamment dans le cadre de la politique de recouvrement[1] de données mise en œuvre au sein de l'Entité.

L'Utilisateur ne fait pas usage des moyens d'authentification ou des droits d'accès d'une tierce personne. De la même façon, il n'essaie pas de masquer sa propre identité.

L'Utilisateur ne fait usage de ses droits d'accès que pour accéder à des informations ou des services nécessaires à l'exercice des missions qui lui ont été confiées et pour lesquels il est autorisé :

- il s'interdit d'accéder ou de tenter d'accéder à des ressources du système d'information pour lesquelles il n'a pas reçu d'habilitation explicite ;
- il ne connecte pas aux réseaux locaux de l'Entité – quelle que soit la nature de ces réseaux (filaires ou non filaires) - des matériels autres que ceux confiés ou autorisés par la direction ou l'Entité ;
- il n'introduit pas des supports de données (clé USB, CDROM, DVD, etc.) sans respecter les règles de l'Entité et prend les précautions nécessaires pour s'assurer de leur innocuité ;
- il n'installe pas, ne télécharge pas ou n'utilise pas, sur le matériel de l'Entité ou sur du matériel personnel utilisé à des fin professionnelles, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou interdits par l'Entité ;
- il s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou du logiciel.

L'Utilisateur informe les administrateurs de toute évolution de ses fonctions nécessitant une modification de ses droits d'accès.

---

[1] Le recouvrement est le dispositif de secours permettant à une personne habilitée d'accéder à des données lorsque le mécanisme principal n'est plus utilisable (perte de mot de passe par exemple)

Protection des équipements informatiques

L'Utilisateur protège les équipements mis à sa disposition :

- il applique les consignes de l'équipe informatique issues de la PSSI opérationnelle de l'Entité afin de s'assurer notamment que la configuration de son équipement suit les bonnes pratiques de sécurité (application des correctifs de sécurité, chiffrement, etc.) ;
- il utilise les moyens de protection disponibles (câble antivol, rangement dans un tiroir ou une armoire fermant à clé, etc.) pour garantir la protection des équipements mobiles et des informations qu'ils renferment (ordinateur portable, clé USB, smartphones, tablettes, etc.) contre le vol ;
- en cas d'absence, même momentanée, il verrouille ou ferme toutes les sessions en cours sur son poste de travail ;
- il signale le plus rapidement possible au chargé de la sécurité des SI (chargé de la SSI au sein de l'Entité ou le cas échéant responsable SSI de la délégation régionale) toute perte, tout vol ou toute compromission suspectée ou avérée d'un équipement mis à sa disposition.

L'Utilisateur protège les équipements personnels qu'il utilise pour accéder, à distance ou à partir du réseau local d'une Entité, aux SI du CNRS ou stocker des données professionnelles en respectant les règles édictées par le CNRS et l'Entité.

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

Protection vis-à-vis des échanges sur les réseaux

Adresse électronique

Le CNRS s'engage à mettre à la disposition de l'Utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative se fait sous la responsabilité de l'Utilisateur.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

Contenu des échanges sur les réseaux

Les échanges électroniques (courriers, forums de discussion, messagerie instantanée, réseaux sociaux, partages de documents, voix, images, vidéos, etc.) respectent la correction normalement attendue dans tout type d'échange tant écrit qu'oral.

La transmission de données classifiées de défense est interdite sauf dispositif spécifique agréé et la transmission de données sensibles doit être réalisée suivant les règles de protection en vigueur.

Vigilance

L'Utilisateur fait preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes, hameçonnage, ...).

Statut et valeur juridique des informations échangées

Les informations échangées par voie électronique avec des tiers peuvent, au plan juridique, former un contrat sous certaines conditions ou encore être utilisés à des fins probatoires.

L'Utilisateur doit, en conséquence, être prudent sur la nature des informations qu'il échange par voie électronique au même titre que pour les courriers traditionnels.

Stockage et archivage des informations échangées

L'Utilisateur est informé que le courriel est un document administratif reconnu en tant que preuve en cas de contentieux.

Protection vis-à-vis de l'accès aux services en ligne sur Internet

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

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

Certains sites malveillants profitent des failles des navigateurs pour récupérer les données présentes sur le poste de travail. D'autres sites mettent à disposition des logiciels qui, sous une apparence anodine, peuvent prendre le contrôle de l'ordinateur et transmettre son contenu au pirate à l'insu de l'Utilisateur. Enfin, certains sites ne fournissent aucune garantie sur l'utilisation ultérieure qui pourra être faite des données transmises. Par conséquent, l'Utilisateur :

- évite de se connecter à des sites suspects ;
- évite de télécharger des logiciels dont l'innocuité n'est pas garantie (nature de l'éditeur, mode de téléchargement, etc.) ;
- n'opère les sauvegardes de données, les partages d'information, les échanges collaboratifs, que sur des sites de confiance, mis à disposition par l'établissement et dont la sécurité a été vérifiée par l'établissement (via par exemple un audit de sécurité) ;
- chiffre les données non publiques qui seraient stockées sur des sites tiers ou transmises via des messageries non sécurisées.

Publication d'informations sur Internet

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

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

Le chargé de la SSI de l'Entité ou le responsable SSI de la délégation dont il relève apporte son soutien à l'Utilisateur pour la mise en œuvre de l'ensemble de ces mesures.

II. Vie privée et ressources informatiques personnelles

Vie privée résiduelle

Les ressources informatiques (poste de travail, serveurs, applications, messagerie, Internet, téléphone, etc.) fournies à l'Utilisateur, par le CNRS ou ses partenaires, EPST, université, etc. - sont réservées à l'exercice de son activité professionnelle.

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

- qu'il reste de courte durée pendant les heures de travail au bureau ;

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

Toute donnée est réputée professionnelle à l'exception des données explicitement désignées par l'Utilisateur comme ayant un caractère privé (par exemple en indiquant la mention « privé » dans le champ « objet » des messages).

L'Utilisateur procède au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet ou en mentionnant le caractère privé sur la ressource utilisée. Cet espace ne doit pas contenir de données à caractère professionnel et il ne doit pas occuper une part excessive des ressources. La protection et la sauvegarde régulière des données à caractère privé incombent à l'Utilisateur.

Ressources informatiques personnelles

Les ressources informatiques personnelles (ordinateurs, smartphones, tablettes, etc. achetés sur des crédits personnels), lorsqu'elles sont utilisées pour accéder aux SI du CNRS, ne doivent pas remettre en cause ou affaiblir, les politiques de sécurité en vigueur dans les Entités par une protection insuffisante ou une utilisation inappropriée.
Lorsque ces ressources informatiques personnelles sont utilisées pour accéder, à distance ou à partir du réseau local d'une Entité, aux SI du CNRS ou stocker des données professionnelles, ces ressources sont autorisées et sécurisées suivant les directives issues de la PGSI et déclarées au service informatique qui gère le parc matériel de l'Entité. Les personnels qui souhaiteraient faire l'acquisition de tels matériels prennent préalablement conseil auprès de leur service informatique.

Gestion des départs

L'Utilisateur est responsable de son espace de données à caractère privé et il lui appartient de le détruire au moment de son départ. En cas de circonstances exceptionnelles (départ impromptu ou décès) le CNRS ne conserve les espaces de données à caractère privé présents sur les ressources informatiques fournies par le CNRS que pour une période de 3 mois maximum (délai permettant à l'Utilisateur ou ses ayants droits de récupérer les informations qui s'y trouvent).

Les données professionnelles restent à la disposition de l'employeur. Les mesures de conservation des données professionnelles sont définies au sein de l'Entité.

III. Respect de la loi informatique et libertés

Si, dans l'accomplissement de ses missions, l'Utilisateur constitue des fichiers contenant des données à caractère personnel soumis aux dispositions de la loi informatique et libertés, il en informe le directeur d'unité afin que les déclarations nécessaires puissent être réalisées auprès du Correspondant Informatique et Libertés (CIL) du CNRS.

IV. Respect de la propriété intellectuelle

L'Utilisateur ne reproduit pas, ne télécharge pas, ne copie pas, ne diffuse pas, ne modifie pas ni n'utilise les logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

V. Impact des droits et devoirs spécifiques aux administrateurs des SI sur les données des utilisateurs

La loi et les règlements [2]imposent au CNRS de garder un historique des accès réalisés par les agents. Le CNRS a donc mis en place une journalisation des accès, conformément aux règles énoncées dans la PGSI et à la déclaration réalisée auprès de la CNIL en application de la loi n°78-17 du 6 janvier 1978 modifiée.

L'administrateur a accès aux traces laissées par l'Utilisateur lors de ses accès sur l'ensemble des ressources informatiques mises à sa disposition par l'Entité ainsi que sur les réseaux locaux et distants.

Ces traces (appelées également « fichiers de journalisation » ou « journaux ») sont sauvegardées 12 mois au maximum.

Les administrateurs peuvent, en cas de dysfonctionnement technique, d'intrusion ou de tentative d'attaque sur les systèmes informatiques utiliser ces traces pour tenter de retrouver l'origine du problème.

Ces personnels sont soumis à une obligation de confidentialité. Ils ne peuvent donc divulguer les informations qu'ils sont amenés à connaitre dans le cadre de leur fonction, en particulier lorsqu'elles sont couvertes par le secret des correspondances ou relèvent de la vie privée de l'utilisateur, dès lors que ces informations ne remettent pas en cause ni le bon fonctionnement technique des applications, ni leur sécurité.

Ils peuvent prendre connaissance ou tenter de prendre connaissance du contenu des répertoires, fichiers ou message manifestement et explicitement désignés comme personnels qu'en présence de l'agent et avec son autorisation expresse, en cas d'urgence justifiée ou de nécessité vis-à-vis de la législation et de la sécurité.

VI. Respect de la loi

L'Utilisateur est tenu de respecter l'ensemble du cadre légal lié à l'utilisation des systèmes d'information, ainsi que toute autre règlementation susceptible de s'appliquer.

En particulier, il respecte :

► la loi du 29 juillet 1881 modifiée sur la liberté de la presse. L'Utilisateur ne diffuse pas des informations constituant des atteintes à la personnalité (injure, discrimination, racisme, xénophobie, révisionnisme, diffamation, obscénité, harcèlement ou menace) ou pouvant constituer une incitation à la haine ou la violence, ou une atteinte à l'image d'une autre personne, à ses convictions ou à sa sensibilité ;

► la règlementation relative au traitement des données à caractère personnel (notamment la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés) ;

► la législation relative aux atteintes aux systèmes de traitement automatisé de données (art. L 323-1 et suivants du code pénal) ;

► la loi n° 94-665 du 4 aout 1994 modifiée relative à l'emploi de la langue française ;

► la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;

---

[2]En particulier l'article 6-II de la Loi pour la Confiance Numérique (LCEN) du 21 juin 2004 qui impose aux fournisseurs d'hébergement et aux fournisseurs d'accès internet de conserver les données d'identification pour les connexions à leurs services et l'article L.34-1 du Code des postes et des communications électroniques (CPCE) qui impose une obligation de conservation de ces données

► les dispositions du code de la propriété intellectuelle relatives à la propriété littéraire et artistique. L'Utilisateur ne fait pas de copies illicites d'éléments (logiciels, images, textes, musiques, sons, etc.) protégés par les lois sur la propriété intellectuelle ;

► les dispositions relatives au respect de la vie privée, de l'ordre public, du secret professionnel.

► les dispositions relatives à la Protection du Potentiel Scientifique et Technique de la Nation.

Certaines de ces dispositions sont assorties de sanctions pénales.

Charte pour l'utilisation des ressources informatiques de l'Université Claude –Bernard Lyon1

Vu le code de l'éducation
Vu le code de la propriété intellectuelle
Vu le code pénal
Vu la délibération du Conseil d'Administration de l'Université Claude Bernard Lyon 1 du 26 novembre 2002
Vu l'avis du Groupe de Travail Structure du 19 novembre 2002
Vu l'avis de la Commission Paritaire d'Etablissement du 24 octobre 2002
Vu l'avis du Conseil Scientifique du 21 octobre 2002
Vu l'avis du Conseil des Etudes et de la Vie Universitaire du 25 avril 2002
Vu l'avis du Conseil d'Administration du Centre de Ressources Informatiques du 14 novembre 2002

PREAMBULE

Le Programme d'Action Gouvernemental vers la Société de l'Information (P.A.G.S.I.) a défini la diffusion d'informations relatives aux administrations et établissements publics par les moyens informatiques comme une mission du service public.
Par ailleurs, le développement des techniques informatiques implique une plus large utilisation de moyens de communications tels quel le courrier électronique ou les listes et forums de discussion.
L'Université Claude –Bernard Lyon 1 s'inscrit dans ces objectifs en développant les moyens informatiques mis à la disposition des étudiants et personnels de l'Université dans le but de renforcer la formation initiale et continue, valoriser le travail de recherche et favoriser le travail universitaire coopératif.
Cette charte définit les conditions générales d'utilisation de ces services dans le cadre des activités relatives aux missions et au fonctionnement de l'Université. Les usages n'entrant pas dans ce cadre précis sont tolérés. Elle a pour objet de rappeler les textes en vigueur et de réglementer le fonctionnement et l'utilisation du système d'information de l'Université.
On entend par système d'information :

- l'ensemble des serveurs : ordinateurs ou autocommutateurs téléphoniques,
- l'ensemble des postes de travail et des terminaux de réseau : ordinateurs fixes ou portables, périphériques, téléphones fixes ou portables.
- l'ensemble des équipements de transmission : concentrateurs, commutateurs, routeurs,
- l'infrastructure de liaison du réseau : faisceaux hertziens, câbles de fibres optiques, câbles UTP ou FTP, locaux techniques,
- l'ensemble des logiciels contenus dans ou faisant fonctionner, inter opérer ou protégeant lesdits ordinateurs et matériels informatiques, y inclus les protocoles de communication permettant :
  - la constitution et la création,
  - l'échange, la circulation, la diffusion,
    de données, fichiers, bases de données,
    intranet, extranet
    images, sons, textes, programmes
    flux quelconques d'information

entre les utilisateurs entre eux ou avec des personnes extérieures.

CHAPITRE I –ACCES AU SYSTEME D'INFORMATION

Article 1 – Définition de l'utilisateur

L'utilisateur est le titulaire d'un compte d'accès tel que défini à l'article 3.
Il s'agit, notamment, des étudiants inscrits dans une formation initiale ou au titre de la formation continue à l'Université Claude –Bernard Lyon 1, des enseignants, chercheurs et personnels administratifs, techniques et de santé de l'Université.

Article 2 – Définition du gestionnaire du système d'information

Le responsable du système d'information de l'Université est désigné gestionnaire du système d'information. Il peut s'agir de plusieurs services. Il veille à la protection, à la maintenance, au bon fonctionnement du système d'information et assure le respect de la présente charte par l'ensemble des utilisateurs et personnels des services informatiques.
Il assure l'exécution de l'ensemble des formalités et déclarations nécessaires, notamment celles issues de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers, et aux libertés, et de la loi du 10 juillet 1991 sur le secret de la correspondance.

Article 3 – Compte d'accès

Un ou plusieurs comptes d'accès sont accordés par le gestionnaire sur l'un quelconque des équipements de l'Université pour favoriser l'accès à l'information scientifique et pour permettre un partage des connaissances et informations relatives aux missions spécifiques de l'Université.
Ce compte d'accès est au minimum concrétisé par l'octroi d'un nom d'utilisateur et d'un mot de passe strictement personnels et confidentiels après acceptation écrite de la charte par l'utilisateur. L'identification de l'utilisateur est obligatoire. Les informations qu'il donne doivent être exactes et actuelles. A défaut, l'ouverture du compte d'accès ne pourra être effective.
L'utilisateur est responsable des opérations effectuées grâce à son identifiant et son mot de passe ; il ne peut les divulguer ou s'approprier ceux d'un autre utilisateur.

Article 4 – Droits de l'utilisateur

Le compte d'accès donne à l'utilisateur un droit d'accès annuel aux services mis à disposition. Ce droit d'accès est personnel, incessible et temporaire. Il fait l'objet d'un renouvellement annuel. Il disparaît dés lors que son titulaire ne répond plus aux critères d'attribution définis à l'article 1 de la charte.
Ce droit d'accès peut être suspendu à tout moment, dés lors qu'est supposé un manquement aux dispositions de la charte de la part de l'utilisateur.
L'utilisateur donne expressément son consentement pour que les données à caractère personnel le concernant soient collectées dans le cadre de l'ouverture du compte d'accès. Ces données ne seront utilisées que pour les finalités de cette inscription.
L'utilisateur peut demander à l'Université la communication des informations nominatives le concernant et les faire rectifier en application des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
L'utilisateur est informé qu'en application des dispositions législatives et réglementaires en vigueur, l'Université est tenue de recueillir et conserver des informations sur les utilisateurs de ses services informatiques et peut, dans le cadre d'une enquête judiciaire, être dans l'obligation de les donner.
En conséquence, tout refus de l'utilisateur relatif à la collecte des informations à caractère personnel demandées implique rejet de la demande de compte d'accès.

Article 5 – Obligations de l'utilisateur

L'utilisateur s'engage à informer immédiatement le gestionnaire de toute perte, de toute tentative de violation ou anomalie relative à une utilisation de son compte d'accès.
L'utilisateur s'engage à effectuer une utilisation rationnelle et loyale des services et, notamment du réseau, de la messagerie et des ressources informatiques afin d'en éviter la saturation et le détournement à des fins personnelles.
L'utilisateur accepte que l'Université puisse avoir connaissance des informations nécessaires à l'administration du réseau (données de volumétrie, incidents, nature du trafic engendré) et puisse prendre toutes mesures urgentes pour stopper la perturbation de ses services. L'Université se réserve, notamment, la possibilité de stopper l'accès aux services en cas d'utilisation excessive ou non conforme à ses missions spécifiques telles que définies dans la présente convention.
L'utilisateur est responsable de l'usage qu'il fait du réseau. Il assure notamment, à son niveau, la sécurité de ce réseau et s'engage à ne pas apporter volontairement de perturbations à son fonctionnement et à mettre en péril l'intégrité des ressources informatiques.
Il s'engage, notamment, à :

- ne pas interrompre le fonctionnement normal du réseau ou des systèmes connectés ;
- ne pas développer, installer ou copier des programmes destinés à contourner la sécurité, saturer les ressources ;
- ne pas introduire des programmes virus, ou contournant la protection des logiciels ;
- ne pas installer de logiciels susceptibles de modifier la configuration des machines sans accord préalable du gestionnaire;
- ne pas s'attaquer aux systèmes d'information de l'université ou de tout autre organisme public ou privé, européen ou étranger, en modifier ou altérer le contenu ;
- ne pas collecter ou tenter de collecter des informations susceptibles d'être utilisées lors de tentatives d'attaques contre des systèmes d'information externes ou internes ;
- ne pas utiliser les ressources informatiques afin de dupliquer, diffuser ou distribuer des logiciels, images, sons et vidéos aux contenus visés par le code pénal ou collectés par des moyens contraires au droit de la propriété intellectuelle, sous quelque forme que ce soit.

Article 6 - Disponibilité du service

L'Université s'efforce, dans la mesure du possible de maintenir accessible le service qu'elle propose de manière permanente mais n'est tenue à aucune obligation d'y parvenir. L'Université peut interrompre l'accès, notamment pour des raisons de maintenance, de mise à niveau et de sécurité sans pouvoir être tenue pour responsable des conséquences de ces interruptions tant à l'égard des utilisateurs que des tiers.

Article 7 – Contrôle et maintenance par le gestionnaire

L'utilisateur est averti que le gestionnaire peut avoir accès à l'ensemble des composants du système d'information, à l'exclusion de la messagerie et des espaces personnels, à n'importe quel moment et ce afin d'effectuer tout acte de protection du système d'information concernant :

- la conservation et sauvegarde, le contrôle de l'absence de diffusion non autorisée d'informations sur les sites web,
- la preuve de la date de création ou de diffusion des dites informations,
- la recherche et le rejet d'intrusions dans le système d'informations ou de matériels violant les règles relatives au droit d'auteur,
- la mise à jour, maintenance, correction et réparation des matériels et logiciels.

Dans le cas où un composant du système d'information ne se trouverait pas dans l'enceinte de l'Université, l'utilisateur qui en a la garde s'oblige à le restituer ou le confier au gestionnaire à la première demande de sa part.

Le gestionnaire pourra mettre en place des outils de contrôle et de surveillance répondant strictement à la finalité de la protection du système d'information.
A cette fin, l'Université dispose des moyens techniques suivants pour procéder à des contrôles de l'utilisation de ses services :

- limitation de l'accès au serveur proxy,
- pare- feux,
- systèmes de détection d'intrusion
- serveur de métrologie

Tout utilisateur peut obtenir auprès du gestionnaire les informations sur les moyens de contrôle mis en œuvre.
Les contrôles techniques qui peuvent être effectués sont justifiés par un souci de sécurité du réseau et/ou des ressources informatiques :
Pour des nécessités de maintenance et de gestion technique, l'utilisation des services et notamment des ressources matérielles et logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment dans le respect des règles relatives à la vie privée. L'Université se réserve le droit, dans le cadre de ces dispositions, de conserver les informations nécessaires à la bonne marche du système.
Le gestionnaire est également en droit de vérifier, sur les seuls services Internet, à l'exclusion de la messagerie, que les contenus diffusés restent conformes aux missions de l'Université.
Le Conseil d'Administration du Centre de Ressources Informatiques (C.A.R.I.) veille au respect des règles en vigueur tant de la part des utilisateurs que des services dépendant du gestionnaire. En particulier, le CARI sera saisi, dès lors que sera soulevé un risque ou constat d'atteinte aux droits des personnes ou aux libertés individuelles qui ne serait pas justifiée par la nature de la tâche à accomplir ni proportionnée au but recherché. De même, le CARI donnera un avis en cas de question soulevée par un personnel du CRI sur les responsabilités encourues dans le cadre de ses interventions.
Le CARI rend compte annuellement auprès du Conseil d'Administration de l'Université de son activité.
Les services techniques peuvent être amenés à effectuer des sauvegardes, y compris sur les contenus personnels, dans le but exclusif d'empêcher des pertes d'informations. Ces contenus ne sont pas accessibles aux tiers sauf procédure juridictionnelle.

Article 8– Antivirus

L'Université dispose d'antivirus. Chaque utilisateur doit se conformer aux instructions de l'Administrateur en ce qui concerne la mise à jour des antivirus.
Seul le gestionnaire est autorisé à introduire dans le système d'information de nouveaux matériels et logiciels. En cas de besoin exprimé par un utilisateur pour un nouveau matériel ou logiciel, il devra demander, à l'Administrateur, une autorisation préalable.
Le non respect de ces dispositions peut exposer l'utilisateur à des sanctions et à la mise en jeu de sa responsabilité en cas d'intrusion, du fait de l'utilisateur, de virus ou d'un tiers non –autorisé dans le système d'information ou de pertes de données.

Article 9 – Pare – feux

L'Université charge le CARI de définir sa politique de sécurité.
Elle dispose de Pare feux (firewall) pour protéger son réseau. Ces équipements ont pour vocation de limiter certains trafics soit en fonction des protocoles utilisés soit en fonction des ports soit en fonction des adresses IP. Le gestionnaire détermine les règles de filtrage à mettre en œuvre afin de garantir un niveau de sécurité optimal en prenant en compte les règles fixées par le CARI. Tout utilisateur pourra faire une demande écrite et justifiée de modification des règles auprès du gestionnaire. Le gestionnaire pourra alors donner suite si cette demande est conforme à la politique de l'Université.
En cas d'urgence, le gestionnaire peut prendre des mesures conservatoires qui devront faire l'objet, postérieurement, d'une validation par le CARI.

CHAPITRE II – UTILISATION DES SERVICES INTERNET

Article 10 – Services mis à disposition

L'Université offre à l'utilisateur, dans la mesure de ses capacités techniques, l'accès Internet avec possibilité de navigation sur le réseau Internet dans son ensemble.

Les services disponibles sur le site de l'Université pourront, notamment, être constitués :

d'un espace d'information pédagogique et scientifique
d'un espace d'information administrative
d'un service de création et d'hébergement de pages personnelles
d'un service de messagerie électronique (Chapitre III de la présente convention)
d'un service de forums
d'un service de discussion en ligne
de listes de diffusion

Article 11 – Capacités techniques

L'Université s'est dotée des moyens lui permettant d'être un fournisseur d'accès.
L'Université s'est dotée des moyens lui permettant d'être un fournisseur d'hébergement Internet.
L'Université s'est dotée des moyens lui permettant de participer à la fourniture de services fournisseur réservés aux établissements d'enseignement supérieur.
L'accès aux services offerts peut avoir lieu :

- soit depuis les sites de l'Université (serveurs, micro-ordinateurs en libre service)
- soit par un accès individuel à partir de toute machine connectée à Internet .

Article 12 – Dispositions législatives et réglementaires

L'utilisateur s'engage à respecter les dispositions législatives et réglementaires en vigueur, notamment :

Celles relatives à la propriété littéraire et artistique, contenues, en particulier, dans le code de la propriété intellectuelle. Le téléchargement de logiciels d'œuvres protégées ou de ressources documentaires électroniques sans autorisation des ayant-droits engage la seule responsabilité de l'utilisateur. L'Administrateur se réserve la possibilité d'effacer du système d'information toute trace de ces logiciels et œuvres.

Celles relatives à l'Informatique, aux fichiers et aux libertés (loi du 6 janvier 1978)
Celles relatives à la protection de la vie privée et du droit à l'image d'autrui.

Par ailleurs, l'utilisateur déclare se soumettre aux règles spécifiques d'utilisation de certaines ressources mises à disposition par l'Université et pour lesquelles il serait informé de l'existence de conditions contractuelles restrictives liant l'Université à des tiers, portant en particulier sur l'utilisation d'œuvres protégées et des ressources documentaires électroniques.
En outre, en application du principe de neutralité commerciale applicable aux Universités, l'utilisateur s'interdit de faire de la publicité sur des produits et services à caractère commercial, dans le cadre de la diffusion d'informations sur des espaces mis à sa disposition sur le site de l'Université.
En application du principe de neutralité politique et religieuse applicable aux universités, l'utilisateur s'interdit toute prise de position sur des sujets politiques généraux ne portant pas directement sur les missions de l'Université et toute manifestation de prosélytisme religieux.
Des espaces d'expression syndicales et associatives seront créés pour permettre la libre expression des opinions des étudiants et personnels en application des dispositions du code de l'éducation.
L'utilisateur s'interdit de produire des contenus à caractère raciste, pornographique, pédophile, injurieux, diffamatoire, incitant à la consommation de substances interdites, à la commission de crimes

ou délits, au suicide ou de nature à porter préjudice, de manière générale à l'image de la communauté universitaire.
L'utilisateur s'interdit, par ailleurs, la consultation ou le téléchargement de documents en provenance de sites illicites, notamment les sites à caractère pédophile ou xénophobe.
Le constat par le gestionnaire de manquements à ces obligations par l'Utilisateur entraîne son exclusion immédiate des services mis à disposition.
Par ailleurs, l'Université dénoncera tout acte délictueux aux autorités judiciaires, et ce, sans préjudice de l'application de sanctions internes à l'Université ou l'Education nationale.

Article 13 – Obligations contractuelles de l'utilisateur

L'utilisateur est autorisé à consulter des sites web à titre privé à la condition que cette navigation n'entrave pas l'accès des autres utilisateurs et ne gêne pas la bonne marche du système d'information en raison, en particulier, de l'encombrement de fichiers téléchargés.

Article 14 – Obligations propres aux personnels de l'Université

La consultation de sites web à titre privé est tolérée dans la mesure où cette navigation n'entrave pas l'accès professionnel et qu'elle ne gêne pas de manière significative la bonne marche du travail de l'utilisateur.

Article 15 – Intranet

L'Intranet fonctionne sous la responsabilité informatique du gestionnaire et sous la responsabilité éditoriale du Chargé de Mission – Communication.
Aucun utilisateur ne peut introduire un élément dans le site ou modifier des éléments produits par l'Université sans l'autorisation du gestionnaire et du Chargé de mission – Communication. Les utilisateurs pourront formuler toute suggestion à ces derniers quant au contenu ou fonctionnement de l'Intranet.
Les personnels seront informés, avant diffusion des données personnelles les concernant, telles que leur adresse professionnelle et leur photographie. Ils pourront demander auprès du gestionnaire à avoir accès à ces données nominatives et demander à ce qu'elles soient rectifiées.

Article 16 – Création de pages personnelles

La mise à disposition de pages s'effectue selon une procédure de demande écrite auprès du gestionnaire. Cette demande devra comporter les nom, prénom, adresse, qualité de l'utilisateur et devra préciser l'objet de sa demande. Le gestionnaire dispose du droit de rejeter toute demande imprécise ou ne correspondant pas aux missions de l'Université.
L'utilisateur s'engage, outre au respect des dispositions de la présente charte et, notamment son article 9, à être attentif à ne pas créer de liens avec des sites illicites ou dont le contenu serait incompatible avec les missions de l'Université.
L'utilisateur est informé qu'il est tenu de ne mettre à disposition sur ses pages que des données libres de droits au titre de la propriété intellectuelle et insusceptibles d'une protection au titre de la loi ou de conventions ou en raison du caractère personnel des données fournies.
L'utilisateur engage seul sa responsabilité au titre des manquements à ses obligations.
Par ailleurs, il est rappelé que les personnels de l'Université ont, dans le cadre de leurs fonctions, une obligation générale de réserve et de protection des données personnelles et confidentielles dont ils pourraient avoir connaissance.

L'utilisateur est informé qu'il lui appartient d'assurer la protection des données sur lesquelles il disposerait d'un droit au titre de la propriété intellectuelle, en particulier en informant les autres utilisateurs du caractère incessible du contenu diffusé.
L'Université ne saurait faire l'objet de poursuites et de réclamations du fait de la copie et de la diffusion par des tiers des contenus des pages personnelles diffusées par les utilisateurs.

Article 17 – Participation à des forums et des services de discussion

L'utilisateur s'oblige à un usage loyal de ces services en s'interdisant l'emploi d'un pseudonyme.
L'utilisateur ne saurait engager l'Université du fait de prises de positions ou de diffusions d'informations illicites sur ces services.
Le gestionnaire se réserve le droit de supprimer tout message litigieux, et ce, sans information préalable de l'utilisateur.

CHAPITRE III – UTILISATION DE LA MESSAGERIE ELECTRONIQUE

Article 18 – Adresse électronique

Chaque utilisateur dispose d'une messagerie électronique composée de son prénom et de son nom. En cas d'homonymie, le gestionnaire fixera la règle d'attribution. L'utilisation d'un pseudonyme ou l'usage d'un faux nom est expressément prohibé, sauf autorisation du gestionnaire qui s 'assurera du bien-fondé de cette utilisation.

Article 19 – Utilisation de la messagerie

L'usage privé de la messagerie (envoi et réception de messages) devra gêner le moins possible le trafic normal de messages professionnels, et ce en termes de volume et de taille des messages échangés et de format des pièces jointes.
Le gestionnaire peut limiter le format, le type et la taille des messages électroniques, y compris les pièces-jointes, envoyés, notamment par note de service. Les messages non conformes à ces limitations ou comportant un virus ne seront pas distribués.
Les messages électroniques ne seront conservés sur le serveur que pour une durée courte déterminée par le gestionnaire mais ne pouvant excéder six mois. Au-delà de cette date les messages seront effacés sauf demande écrite de l'utilisateur acceptée par le gestionnaire L'Université ne garantit pas que le service de messagerie sera exempt de toute interruption, retard, incident de sécurité ou erreur.
L'Université ne garantit pas les résultats pouvant être obtenus à l'aide de ce service, ni la précision ou la fiabilité des informations acquises par son intermédiaire.
L'utilisateur est informé que l'Université n'exerce aucune surveillance ni aucun contrôle éditorial sur les messages envoyés et reçus. L'Université ne pourra, de ce fait, être tenue pour responsable de ces contenus.

Article 20 – Messages de service

Malgré son extrême facilité d'utilisation, une attention toute particulière doit être portée à leur rédaction et leur diffusion. Le message électronique est un écrit pouvant engager l'Université ; il peut être reconnu comme un commencement de preuve pour établir un fait ou un acte juridique. Les règles hiérarchiques et de délégations de signature devront impérativement être respectées. Aucun message électronique ne devra être envoyé à un tiers aux services sans autorisation de l'autorité ayant pouvoir de décision.
A ce titre, une messagerie électronique nominative sera ouverte par personnel. L'accès à cette messagerie est strictement personnel. Parallèlement, un alias fonctionnel sera attribué par service. Seul le numéro de cet alias sera signalé dans les courriers et les annuaires concernant les services.
Les utilisateurs de cet alias sont informés que les contenus que la messagerie véhicule peuvent faire l'objet d'un contrôle de la part du chef de service ou des services informatiques dans le cadre de leur mission de sécurisation du réseau.
Par ailleurs, les risques d'interception de messages électroniques exigent de limiter l'utilisation de la messagerie électronique à destination de l'extérieur du Système d'information aux informations à caractère non confidentiel, non stratégique et non sensible sauf cryptage assuré en accord avec le gestionnaire selon les règles en vigueur.

Article 21 – Dispositions propres aux personnels de l'Université

L'Université reconnaît, en application des dispositions du code du travail, que le salarié a droit au respect de sa vie privée, même pendant le temps de service et sur le lieu de travail ; celle-ci implique le secret de ses correspondances et de ses contenus personnels.
L'utilisateur porte l'entière responsabilité des messages personnels transmis par le biais de cette messagerie. Tout usage illicite ou abusif peut entraîner la suppression immédiate de l'accès à la messagerie personnelle.
Par ailleurs, l'utilisateur s'attachera à conserver sur son poste de travail les éventuelles correspondances privées qu'il serait amené à conserver dans un fichier spécifique portant son nom et la mention «correspondance privée ».

CHAPITRE IV – SANCTIONS

Article 22 – Sanctions applicables aux étudiants

Outre les sanctions pénales contenues dans le code pénal, les étudiants encourent, en cas de non respect des dispositions de la présente convention des sanctions disciplinaires.
Ces sanctions sont décidées par le Président après étude du dossier par la section disciplinaire de l'Université prévue à l'article L 712-4 du code de l'éducation.
Le droit d'accès peut être définitivement retiré si le manquement est dûment constaté par la section disciplinaire.
Les sanctions encourues sont fixées par le décret n° 92-657 du 13 juillet 1992 modifié fixant la procédure disciplinaire dans les Etablissements Publics à caractère Scientifique, Culturel et Professionnel (EPSCP).

Article 23 – Sanctions applicables aux personnels

Outre les sanctions pénales contenues dans le code pénal, les enseignants et enseignants – chercheurs encourent, en cas de non respect des dispositions de la présente convention des sanctions

disciplinaires. Ces sanctions sont décidées par la section disciplinaire de l'Université prévue à l'article L 712-4 du code de l'éducation.
Les sanctions encourues sont fixées par le décret n° 92-657 du 13 juillet 1992 modifié fixant la procédure disciplinaire dans les EPSCP.
Les sanctions encourues par les autres personnels sont déterminées par chacune des dispositions réglementaires ou statutaires les concernant.

CHAPITRE V – FORMALITES

Article 24 – Consultation des instances de l'Université

Avant la mise en place de la présente charte, ont été consultés :

- le Conseil des Etudes et de la Vie Universitaire sur les dispositions relatives à la vie étudiante.
- Le Conseil Scientifique eu égard à ses compétences scientifiques
- la CPE sur les dispositions relatives aux personnels.
- le CARI sur l'ensemble de ses dispositions

Les propositions ultérieures de modification seront portées devant ces instances en tant qu'elles les concernent avant adoption par le Conseil d'Administration de l'Université.

Article 25 – Affichage et formalités

La présente charte sera affichée dés son adoption par le Conseil d'Administration et sera accessible sur l'Internet et l'Intranet de l'Université. Des extraits de cette charte seront diffusées auprès des étudiants et des personnels.

RENATER
CONNECTEUR DE SAVOIRS

Version: 2014

Charte déontologique RENATER

1. La présente Charte déontologique définit les règles d'usage qui s'imposent à tout utilisateur du Réseau RENATER[1].

2. Le réseau RENATER est un réseau qui, par nature, recèle des risques dont l'Etablissement Signataire est informé. Il est nécessairement utilisé sous la responsabilité du Signataire.

   Il appelle pour son bon usage et sa sécurité, une coopération entre les utilisateurs. Celle-ci repose notamment sur l'engagement de l'Etablissement Signataire, au nom des utilisateurs de son/ses Sites[2] ayant accès directement ou indirectement au réseau RENATER, à veiller à :

   - une utilisation à des fins strictement professionnelles conforme à la finalité du réseau RENATER : enseignement, recherche, développements techniques, transfert de technologies, diffusion d'informations scientifiques, techniques et culturelles, expérimentations de nouveaux services présentant un caractère d'innovation technique (voir annexe 1, point 1) ;

   - une utilisation rationnelle des ressources du réseau RENATER de manière à éviter toute consommation abusive de ces ressources, notamment en soumettant à l'agrément préalable du GIP RENATER la mise en oeuvre d'applications qui engendrent un trafic permanent (voir annexe 1, point 2) ;

   - une utilisation loyale des ressources du réseau RENATER en prévenant et s'abstenant de toute utilisation malveillante destinée à perturber ou porter atteinte au réseau RENATER (voir annexe 1, point 3) ;

---

[1] L'expression "réseau RENATER" désigne l'ensemble des réseaux ou nœuds de communication délivrant directement ou indirectement, sur le territoire national, aux sites agréés, tout ou partie des services pour lesquels le GIP RENATER est maître d'ouvrage, quel qu'en soit l'opérateur ou le maître d'œuvre.

[2] Le(s) Site(s) du Signataire désigne(nt) le ou les sites à l'intérieur duquel/desquels toutes les entités (bâtiments, étages, locaux etc.) reliées, directement ou indirectement, au réseau RENATER relèvent de la personne morale représentée par le Signataire de la présente Charte.

- véhiculer et mettre à disposition sur le réseau seulement des données licites au regard des lois qui leur sont applicables (voir annexe 1, point 4 et annexe 4 : liste informative et non exhaustive pour ce qui concerne les lois françaises) ;

- ne pas donner accès à titre commercial ou non, rémunéré ou non, au réseau RENATER à des tiers non autorisés sans l'accord préalable et exprès du GIP RENATER (voir annexe 1, point 5) ;

- mettre en oeuvre les ressources techniques et humaines requises pour assurer un niveau permanent de sécurité conforme à l'état de l'art et aux règles en vigueur dans ce domaine et pour prévenir les agressions éventuelles à partir ou par l'intermédiaire de son/ses Sites (voir annexe 2) ; la nature des données véhiculées ou mises à disposition sur le réseau peut déterminer, à l'initiative et sous la responsabilité du Signataire, un niveau de sécurité particulier qu'il lui appartient de mettre en oeuvre ;

- plus généralement, à se conformer à la présente Charte.

3. Le Signataire de la Charte est informé et accepte expressément que le GIP RENATER procède à des contrôles de la bonne utilisation du réseau RENATER (voir annexe 3) et qu'en cas de manquement à ses obligations telles qu'énoncées à l'article 2 ci-dessus ou, le cas échéant, à la demande de l'autorité de tutelle du ou des Site(s) concerné(s), le GIP RENATER suspende l'accès au réseau RENATER, au niveau national ou international de son ou ses Sites concerné(s).

4. Le Signataire accepte que le GIP RENATER prenne des mesures d'urgence, y inclus la décision de limiter ou d'interrompre temporairement pour le(s) Site(s) concerné(s) l'accès au réseau RENATER au niveau régional, national ou international, pour préserver la sécurité en cas d'incident dont le GIP RENATER aurait connaissance.

   Toutefois, ces mesures :

   - seront accompagnées dans les meilleurs délais d'un dialogue avec le Correspondant de Sécurité du ou des Site(s) concerné(s) ;

   - et ne pourront être mises en oeuvre que dans le cadre d'une procédure approuvée par le conseil d'administration du GIP RENATER et sous réserve de leur faisabilité technique et juridique ;

   - et sur décision des responsables sécurité désignés par les membres fondateurs du GIP RENATER.

   Dans le cas où le(s) Site(s) seraient victime(s) d'actions malveillantes répétées de la part d'un autre Site, sur demande du Signataire du Site ou des Site(s) concerné(s), le GIP RENATER s'engage à mettre en oeuvre les mesures de restriction dans les mêmes termes et conditions que ci-dessus.

5. Le Signataire est informé et accepte expressément que le GIP RENATER modifie la présente Charte notamment pour tenir compte des évolutions législatives à intervenir dans ce domaine ; ces modifications lui seront notifiées périodiquement.

6. Le Signataire de la présente Charte, représentant de la personne morale du ou des Site(s) (nom, prénom, fonction)

reconnaît avoir pris connaissance de la présente Charte de déontologie du Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche RENATER, et s'engage à les respecter et les faire respecter par tous ses utilisateurs raccordés au réseau RENATER par l'intermédiaire de la prise RENATER du Site ou des Sites identifié(s) sur le Feuillet Services RENATER ou de tous les autres sites qui aurai(en)t accès au réseau RENATER dans le cadre d'une Convention Financière établie à cet effet entre le Signataire et le GIP RENATER.
La personne morale désigne un Correspondant Sécurité (Annexe 2).

Date :
Signature :
Cachet :

Annexe 1

1. Utilisation à des fins strictement professionnelles du réseau RENATER.

Le réseau RENATER est destiné à véhiculer le trafic engendré par des activités d'enseignement, recherche, développements techniques, transfert de technologies, diffusion d'informations scientifiques, techniques et culturelles, expérimentations de nouveaux services présentant un caractère d'innovation technique.

Les activités d'administration et de gestion des centres de recherche, de développement ou d'enseignement sont assimilées à la recherche ou à l'enseignement.

Les autres activités, notamment vente de services doivent faire l'objet d'un accord préalable et écrit du GIP RENATER, à l'exclusion toutefois des activités commerciales liées à l'enseignement, à la recherche et au développement technique ainsi qu'aux transferts de technologie et à la diffusion d'informations scientifiques, techniques et culturelles.

2. Utilisation rationnelle du réseau RENATER

Pour offrir à l'ensemble des utilisateurs un niveau de qualité optimale, le GIP RENATER limite l'utilisation d'applications consommatrices de ressources de réseau (diffusion de vidéo notamment). Dans ces conditions, la mise en oeuvre d'applications qui engendrent un trafic permanent est soumise à l'accord préalable et écrit du GIP RENATER. Les limitations pourront porter sur des créneaux horaires, ou sur l'utilisation des liaisons nationales ou internationales particulièrement chargées.

Pour ne pas pénaliser le développement et l'expérimentation de ces applications, le GIP RENATER cherchera à en assurer la coordination de mise en oeuvre.

3. Utilisation loyale du réseau RENATER

Le Signataire s'engage à veiller à ce qu'aucun utilisateur sur son/ses Sites ne crée(nt) ou ne génère(nt) sciemment des données ayant pour effet de saturer les liaisons du réseau RENATER ou encore d'épuiser les ressources de ses équipements. En particulier, les automates à base de requêtes ICMP sur les routeurs du réseau RENATER sont interdits, sauf accord préalable et écrit du GIP RENATER.

4. Licité des données véhiculées sur le réseau RENATER

Les données véhiculées et mises à disposition sur le réseau à l'initiative des utilisateurs du réseau RENATER doivent être licites. A ce titre, les utilisateurs doivent respecter l'ensemble des dispositions légales, notamment :

- le Code de la Propriété Intellectuelle qui fait interdiction d'utiliser, de reproduire et plus généralement d'exploiter des oeuvres protégées par le droit d'auteur, notamment les logiciels, sans l'autorisation de l'auteur ou du titulaire des droits.
- le Nouveau Code Pénal qui sanctionne les atteintes à la personnalité et aux mineurs ainsi que les crimes et délits technologiques.
- la loi du 29 juillet 1881 modifiée, sanctionnant les infractions de presse, notamment la diffamation, le négationnisme, le racisme et les injures.
- la loi sur la cryptologie (loi n° 2004-575 du 21 juin 2004)

Une annexe informative du dispositif légal en vigueur est jointe à la présente Charte en Annexe 4.

5. Fourniture d'accès indirect au réseau RENATER.

Les Sites font l'objet d'une procédure d'agrément (voir feuillet d'agrément) . L'accès au réseau RENATER est réservé aux seuls utilisateurs des Sites agréés et à eux seuls. A ce titre, tout accès à titre commercial ou non, rémunéré ou non à des tiers non autorisés est interdit sauf accord préalable et écrit du GIP RENATER. Il est également interdit d'offrir des accès par le réseau commuté ou numéris à des individus qui ne sont pas utilisateurs du ou des Sites. Il appartient au Signataire d'identifier et de contrôler les accès. Le Signataire engage à ce titre sa responsabilité propre.

Les accès indirects concernent également la retransmission ou le relais de services d'informations obtenus à travers le réseau RENATER.

Le raccordement au réseau RENATER d'autres réseaux, nationaux, étrangers, internationaux, ou prestataires de services commerciaux, par l'intermédiaire d'un Site agréé est sujet à l'accord préalable du GIP RENATER. Il devra faire l'objet d'une procédure d'agrément.

Toutefois lorsqu'un Site fait partie d'une communauté ou d'une entreprise (centre de recherche industriel au sein d'une entreprise, école dépendant d'une chambre de commerce, service d'enseignement et laboratoire de recherche universitaires au sein d'un centre hospitalier universitaire....), et que son réseau est connecté à des réseaux de cette communauté ou de cette entreprise, le Signataire a pour seules obligations :

- de ne pas donner accès au réseau RENATER aux utilisateurs des réseaux de cette communauté ou de cette entreprise ;
- d'informer le responsable de ces réseaux de la teneur de la présente Charte qui implique que les utilisateurs de ces réseaux ne peuvent accéder à Renater;
- de prendre toutes mesures d'isolement ou de filtrage de ces réseaux, s'ils sont directement ou indirectement à l'origine d'incidents sur le réseau RENATER.

Annexe 2
Sécurité

Le Signataire, seul responsable de la sécurité de ses équipements, s'engage à mettre en oeuvre une politique de sécurité d'un niveau conforme à l'état de l'art et aux règles en vigueur dans ce domaine.

A ce titre, il appartient au Signataire de mettre en oeuvre les ressources techniques et humaines requises pour protéger son ou ses Site(s) et pour éviter les agressions contre d'autres sites connectés au réseau RENATER ou à d'autres réseaux ou encore contre le réseau RENATER à partir ou par l'intermédiaire de son ou de ses Site(s). Des informations sur ce sujet sont accessibles sur le site Web de Renater. Il est demandé au Signataire de veiller tout particulièrement aux accès à leur(s) Site(s) par le réseau commuté ou par le réseau Numéris.

Par ailleurs, il appartient au Signataire de désigner une personne dénommée « Correspondant Sécurité » et de faire assurer la formation et l'information des utilisateurs du ou de ses Sites.

Le Correspondant Sécurité :

Pour ce qui concerne les événements liés à la sécurité, le Correspondant Sécurité doit disposer de tous les pouvoirs opérationnels nécessaires pour intervenir efficacement et dans les meilleurs délais, en cas d'incident de sécurité, notamment à la demande du GIP RENATER, tant au niveau de la connexion du ou des Sites agréés du Signataire que sur les éventuelles connexions directes vers d'autres sites.

Lorsqu'un incident de sécurité se produit sur le(s) Site(s) du Signataire, de nature à impliquer un ou plusieurs autres Sites et/ou le réseau RENATER, le Correspondant Sécurité du Site concerné doit informer le GIP RENATER dans les meilleurs délais, et, au besoin, dans la mesure de son possible, prévenir les autres sites et apporter son concours à la solution de l'incident.

Le devoir d'information et de formation des Utilisateurs.

Le Signataire s'engage à informer les utilisateurs, notamment les administrateurs de systèmes informatiques, de son/ses Site(s) de la teneur de la présente Charte, à s'assurer qu'ils en ont effectivement pris connaissance, et à demander aux directions des autres sites ayant accès au réseau RENATER via son propre Site de faire la même démarche. A cet effet, il est conseillé de faire signer par les utilisateurs une déclaration indiquant qu'ils en ont pris connaissance.

Par ailleurs, le Signataire s'engage à mettre en oeuvre les actions de formation nécessaires.

Annexe 3

Le Signataire accepte que le GIP RENATER puisse vérifier la bonne utilisation par les utilisateurs de son/ses Site(s) du réseau RENATER. A cet effet, il accepte que le GIP RENATER ait accès, notamment auprès des opérateurs concernés, aux informations d'administration de réseau (telles que des données de volumétrie, d'incidents, etc...) concernant son/ses Site(s). Elles seront considérées par le GIP RENATER comme confidentielles, et seuls des bilans de synthèse globaux pourront être rendus publics en dehors de l'accord explicite du Signataire ou, le cas échéant, de son autorité de tutelle.

Le Signataire reconnaît que les conditions de confidentialité de ces informations figurant éventuellement dans le (ou les) contrat(s) qu'il a signé(s) avec l'opérateur lui donnant directement ou indirectement accès à RENATER ne sont pas opposables, ni par lui ni par l'opérateur, à la communication d'informations définie ci-dessus.

Annexe 4

Liste informative des infractions susceptibles d'être commises

1. **Infractions prévues par le Nouveau Code pénal**

1.1. **Crimes et délits contre les personnes**

- **Atteintes à la personnalité:**

(Respect de la vie privée art. 9 du code civil)

- Atteintes à la vie privée (art. 226-1 al. 2 ; 226-2 al. 2, art.432-9 modifié par la loi n° 2004-669 du 9 juillet 2004)
- Atteintes à la représentation de la personne (art. 226-8)
- Dénonciation calomnieuse (art. 226-10)
- Atteinte au secret professionnel (art. 226-13)
- Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques (art. 226-16 à 226-24, issus de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

- **Atteintes aux mineurs**: (art. 227-23 ; 227-24 et 227-28).

Loi 2004-575 du 21 juin 2004 (LCEN)

1.2. **Crimes et délits contre les biens**

- Escroquerie (art. 313-1 et suite)
- Atteintes aux systèmes de traitement automatisé de données (art. 323-1 à 323-7 modifiés par la loi n° 2004-575 du 21 juin 2004).

1.3 **Cryptologie**

- Art. 132-79 (inséré par loi n° 2004-575 du 21 juin 2004 art. 37)

2. **Infractions de presse (loi 29 juillet 1881, modifiée)**

- Provocation aux crimes et délits (art.23 et 24)
- Apologie des crimes contre l'humanité (art. 24)
- Apologie et provocation au terrorisme (art. 24)
- Provocation à la haine raciale (art. 24)
- « Négationnisme »: contestation des crimes contre l'humanité (art. 24 bis)
- Diffamation (art. 30.31 et 32)
- Injure (art. 33)

3. **Infraction au Code de la propriété intellectuelle**

- Contrefaçon d'une oeuvre de l'esprit (y compris d'un logiciel) (art. 335-2 modifié par la loi n° 2004-204 du 9 mars 2004, art. 34 - et art. 335-3)
- Contrefaçon d'un dessin ou d'un modèle (art. L521-4 modifiée par la loi n° 2004-204 du 9 mars 2004, art. 34)
- Contrefaçon de marque (art. L716-9 - modifié par la loi n° 2004-204 du 9 mars 2004, art. 34 -et suivants)

4. **Participation à la tenue d'une maison de jeux de hasard (« cyber-casino »)**

- Art.1 de la loi du 12 juillet 1983, modifié par la loi du 16 décembre 1992

ANNEXE N°5 : MODALITES DE SAUVEGARDE DES POSTES DE TRAVAIL INFORMATIQUE

La taille du laboratoire, la volumétrie totale représentée par les postes de travail et la grande hétérogénéité des systèmes d'exploitation utilisés rendent la mise en place d'un service de sauvegarde automatique et centralisé trop complexe et trop coûteuse. Cependant, des infrastructures de stockage communes permettent aux membres du LBBE qui le souhaitent d'effectuer des sauvegardes d'une partie de leurs données :

- le Pôle Informatique administre et met à disposition un espace de sauvegarde sur une baie de disques durs. L'accès à cet espace est soumis à la création d'un compte par le Pôle Informatique sur simple demande. Les sauvegardes s'effectuent par des protocoles réseau de type SSH ou rsync en ligne de commande ou à travers des applicatifs, issus de la communauté des logiciels libres de préférence. Un quota par défaut est attribué à chaque utilisateur et peut être modulé si nécessaire. Un outil accessible par le web permet de visualiser le taux d'occupation de l'espace pour chaque utilisateur. Le serveur et la baie de stockage des sauvegardes sont hébergés dans une salle informatique de l'étage PRABI. L'intégrité des données est assurée par un système de parité de type RAID, qui autorise la défaillance de plusieurs disques durs sans perte de données.

- les membres du laboratoire peuvent avoir accès au système de sauvegarde des postes de travail mis en place par l'université. Celui-ci s'appuie sur un logiciel commercial et un nombre de licences limité est mis à disposition du LBBE par la DSI de l'université. Les demandes de licence se font par le biais du Pôle Informatique. Une fois la licence acquise, l'utilisateur configure et gère ses sauvegardes, dans la limite des quotas qui lui sont imposés.

Ces 2 solutions sont disponibles pour les 3 grandes familles de systèmes d'exploitation, linux, Mac OS et Windows. Compte tenu des limitations en terme d'espace disponible, il n'est pas souhaitable d'utiliser ces systèmes pour une sauvegarde complète des postes, intégrant le système d'exploitation et les logiciels. Il est préférable de réserver ces outils pour la sécurisation des données à caractère scientifique et/ou professionnelles. L'utilisation de l'un ou de ces 2 systèmes de sauvegarde reste sous la responsabilité des utilisateurs et n'est pas incompatible avec des sauvegardes sur des médias mobiles (type disque dur externe).

ANNEXE F : MODALITES D'UTILISATION DES VEHICULES DE SERVICE

En juillet 2018, état du parc automobile du LBBE :

Parc Université Lyon 1	Parc CNRS
Kangoo "blanc" essence - DB460BT	Kangoo "2015" diesel - BQ775WS
	Kangoo "2018" essence – EZ326VV

Cas particuliers du :

- Kangoo "curculio" diesel - AS310GS acheté par S Venner
- Peugeot Boxer acheté par le Labex

Une réunion est organisée **chaque début d'année universitaire** afin de dresser un **planning prévisionnel** d'utilisation des véhicules et d'anticiper les besoins. Un mail sera envoyé au préalable pour que les personnes concernées puissent faire remonter leurs besoins.

Les réservations de plus d'une semaine faites après l'établissement de ce planning annuel devront être validées par le DU.

Après l'utilisation d'un véhicule pour une durée supérieure à un mois ou en conditions de terrain accidenté il sera systématiquement bloqué quelques jours pour une visite de contrôle chez le garagiste.

Le retrait des clés et papier des véhicules se fait auprès d'Odile Mulet-Marquis.

Pour être conducteur·trice, il faut :

- Etre membre de l'unité quel que soit le statut (personnel permanent, non permanent, doctorant, stagiaire),
- Etre muni d'un ordre de mission de son autorité de tutelle autorisant l'utilisation d'un véhicule de service,
- Etre détenteur d'un permis de conduire valide.

L'autorisation de conduire sera immédiatement retirée en cas d'usage anormal ou dangereux du véhicule.
En cas d'infraction au code de la route, le conducteur ou la conductrice du véhicule de service devra s'acquitter des amendes qui lui seraient infligées et subir les éventuelles sanctions pénales.

Pour être passager·ère, il faut être muni d'un ordre de mission de son autorité de tutelle.

MODALITES PRATIQUES D'UTILISATION D'UN VEHICULE

Avant chaque utilisation

- Faire le tour du véhicule pour détecter toute anomalie qui pourrait ne pas avoir été signalée par l'utilisateur·trice précédent·e.
- Vérifier la pression des pneus, le niveau d'huile, le niveau de liquide de refroidissement, les feux de signalisation et les feux de croisements, veilleuse, plein phares, feux de brouillard.

- Remplir le cahier de bord du véhicule en mentionnant : la date, le nom du conducteur ou de la conductrice, le lieu de départ, le kilométrage, la destination….

Au retour de mission

- Chaque utilisateur·trice doit restituer le véhicule **avec le plein de carburant** dans le réservoir.
- Les véhicules doivent être rendus **propres** (intérieur et extérieur). Une « carte lavage » BP, utilisable, entre autres, à la station-service en face de l'Université, est à disposition dans chaque véhicule.
- Remplir le cahier de bord du véhicule sans oublier de signaler tout incident, accident ou anomalie au pôle administratif.

Une **vérification** de la propreté, du niveau d'essence ainsi que du bon état général du véhicule sera effectuée par le pôle administratif en présence de l'utilisateur·trice au moment de la remise des clefs.

Un engagement à respecter l'ensemble de ces règles sera signé par chaque utilisateur·trice et à chaque mise à jour du présent règlement.

Le Directeur d'Unité se réserve le droit de retirer l'autorisation de conduire les véhicules de service en cas de non-respect de ces règles.