Modèle de règlement intérieur d'Unité

PREAMBULE

L'Unité Biogéosciences est une UMR implantée dans les locaux de l'université de Bourgogne.

Le présent règlement intérieur a été soumis à l'avis du Conseil de laboratoire*,* réuni le 09/09/2015

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 de Bourgogne. En cas de contradiction, les dispositions les plus restrictives prévaudront.

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

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

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

SOMMAIRE

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 au moins une fois par an par convocation à tous les membres du laboratoire.

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 18 membres :

- membres de droit : le Directeur d'Unité
- membres nommés : 5
- membres élus : 12

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 de l'avis formulé par la ou les sections du Comité national de la recherche scientifique dont relève l'Unité ;
- le programme de formation en cours et pour l'année à venir ;
- toutes mesures relatives à l'organisation et au fonctionnement de l'Unité et susceptibles d'avoir une incidence sur la situation et les conditions de travail du personnel.

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

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

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

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

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

1-2-3 Fonctionnement

Le Conseil de laboratoire est présidé par le Directeur de l'Unité. Il se réunit au moins trois fois par an. Tous les membres du laboratoire sont informés des réunions du Conseil de laboratoire et des ordres du jour. Seuls les membres du Conseil sont conviés. Le directeur du laboratoire peut inviter des membres du laboratoire qui ne sont pas membre du Conseil à y participer en fonction de l'ordre du jour.

1.3 : Autres : Conseil scientifique, cellule de direction …

Le Comité de Direction de l'Unité est composé du Directeur de l'Unité, du responsable de chaque équipe et d'un membre supplémentaire par équipe. Il prépare les dossiers avant débat au conseil de laboratoire. Il aide le directeur d'unité dans sa gouvernance quotidienne.

1.4 Organisation de l'Unité

Le laboratoire est structuré en quatre équipes de recherche (un organigramme à jour peut être trouvé sur le site Web du laboratoire) :

- équipe Ecologie Evolutive (ECO/EVOL), placée sous la responsabilité de Yannick Moret ;
- équipe Biodiversité, Macroécologie, Evolution (BioME), placée sous la responsabilité de Sophie Montuire ;
- équipe Systèmes, Environnements, et Dynamique Sédimentaire (SEDS), placée sous la responsabilité de Emmanuelle Vennin ;
- équipe Centre de Recherche de Climatologie (CRC), placée sous la responsabilité de Yves Richard.

Les équipes organisent leur animation interne et plus généralement leur vie collective (y compris l'arbitrage des fonds de recherche attribués par le conseil de laboratoire) à leur convenance.

Des plateaux techniques sont constitués afin d'assurer une aide technique aux opérations de recherche. Des comités de pilotages peuvent être constitués pour certains d'entre eux (se référer au responsable du plateau ou de la plateforme : cf. article 8.2). Le laboratoire peut aider financièrement les plateaux et plateformes techniques. Si les dotations financières attribuées par le conseil de laboratoire ne sont pas suffisantes au bon fonctionnement des plateaux, ceux-ci devront trouver des ressources externes, en collaboration avec les chercheurs et enseignants-chercheurs.

Les moyens financiers du laboratoire sont gérés comme suit :

- les ressources obtenues sur appels d'offres (ANR, Région Bourgogne, Europe, Contrats industriels, BQR…) restent à la disposition des porteurs scientifiques des projets, sous la responsabilité du directeur d'unité ;
- les ressources dites de soutien de base sont distribuées aux chercheurs et enseignants-chercheurs, aux doctorants, post-doctorants et ingénieurs de recherche, aux équipes de recherches, aux plateaux et plate-forme techniques et administratives selon des modalités discutées et votées en Conseil de laboratoire.

Le service Gestion / administration assure l'ensemble des opérations globale de gestion et de finance. La gestion de certains contrats de recherche peut être assurée par le service financier de l'UFR SVTE. Dans ce cas, l'engagement des dépenses reste sous la responsabilité du directeur d'unité

L'UMR Biogéosciences dispose d'un site Web (http://biogeosciences.u-bourgogne.fr/fr/) sur lequel la structure de l'unité et les principales informations peuvent être consultées. Le site dispose d'une page pratique à accès restreint aux membres de l'unité contenant un ensemble d'information et de documents téléchargeables relatifs à la vie quotidienne dans l'unité (http://biogeosciences.u-bourgogne.fr/fr/pratique). Le site dispose d'une page de réservation en ligne des salles de réunion, des véhicules et de certains laboratoires ou instruments. Le Webmaster assure la diffusion de codes d'accès aux utilisateurs.

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

Les conditions d'accès aux SI de l'Unité, y compris les SI sensibles relevant de secteurs scientifiques protégés, et de restitution des moyens d'accès aux SI sont définies de façon détaillée par la PSSI opérationnelle applicable à l'Unité (**cf. annexe n° 6**). 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.

Les personnes qui ont accès aux SI de l'Unité doivent, au préalable, avoir pris connaissance de la Charte de la Sécurité des Systèmes d'Information en vigueur dans l'Unité (**cf. annexe n° 5**).

1.6 Accès aux locaux

Les locaux du laboratoire sont situés à l'université de Bourgogne : au 6 boulevard Gabriel, 21000 Dijon. Les modalités d'accès sont celles régies par l'UFR SVTE.

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. Cet accès, en dehors de la plage horaire de référence, ne concerne que le travail de bureau, et en aucun cas le travail dans des services communs (sauf cas particulier des animaleries). 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…).

Heures ouvrables pour l'accès aux bâtiments : de 7h30 heures à 20h00 heures du lundi au vendredi, de 7h30 heures à 14h00 heures le samedi, de 7h30 heures à 18h30 heures pendant les périodes de congés, dans ce cas, une information est envoyée à l'ensemble des membres du laboratoire.

Pour les personnes qui participent directement aux activités scientifiques et techniques de l'Unité (personnels permanents, stagiaires, doctorants, personnes participant à une activité de recherche, en formation, effectuant une prestation de service).

L'accès aux locaux en dehors des heures ouvrables est expressément et nommément autorisé par le Directeur de l'Unité (dans les conditions explicitées ci-dessus).

Le Directeur d'Unité informe le fonctionnaire sécurité défense (FSD) des inscriptions aux formations relevant d'un secteur scientifique et technique protégé dispensé dans l'Unité.

Pour les visiteurs :

Le Directeur d'Unité doit veiller à la mise à jour du répertoire des visites, qui pourra lui être demandé à tout moment.

A leur arrivée, les visiteurs indiquent dans un répertoire leurs nom, prénom, date et lieu de naissance, nationalité, organisme d'appartenance, ainsi que la date et le motif de la visite. Ils fournissent également la preuve de leur identité et une copie de leur assurance responsabilité civile.

Ce répertoire doit faire l'objet d'une déclaration au CIL.

Les visites se font toujours en la présence d'un personnel permanent, généralement la personne qui reçoit la visite.

Au préalable, les sujets qui ne doivent pas être abordés en présence des visiteurs auront été définis.

Les mesures de sécurité de l'Unité sont portées à la connaissance des visiteurs par l'accompagnateur.

Les visites ne peuvent avoir lieu que pendant les heures ouvrables.

En tout état de cause, les interventions justifiées par un risque imminent pour la vie, la sécurité des personnes et des biens ne sont pas soumis aux dispositions relatives à l'accès des visiteurs aux locaux.

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.

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 de l'Université de Bourgogne : la durée annuelle de travail est fixée à 1 607 heures. Cette durée ne tient pas compte des 7 heures de travail dues au titre de la journée de solidarité. Les modalités de mise en œuvre sont indiquées dans le guide de mise en place de l'ARTT à l'Université Bourgogne disponible dans l'Intranet de l'uB et sur décisions des Services Généraux de l'uB et du Directeur de l'UFR SVTE (les modalités d'accomplissement de cette journée sont précisées à l'article 4.3 du présent règlement intérieur).

Pour les personnels relevant d'un établissement qui n'est pas une tutelle du laboratoire : se référer aux règles internes à ces établissements.

Article 3 : Horaires

3.1 : Durée hebdomadaire de travail

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.

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 permanents et de 36h11 pour les personnels non permanents (CDD), conformément aux dispositions de l'article 4 du cadrage national du CNRS
- pour les personnels uB, elle est de 37h30, conformément aux dispositions du guide ARTT de l'uB

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. 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 par jour. Un temps de pause réglementaire de 20 minutes maximum par jour est assimilé à du travail effectif. La plage horaire de travail de référence commence à 7h30 heures et se termine à 20h00 heures les jours ouvrés. La durée quotidienne du travail effectif est minimum de 6 heures et ne peut excéder 10 heures. L'amplitude maximale ne peut excéder 11 heures. Les agents bénéficient d'un repos minimum quotidien de 11 heures consécutives.

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 du guide ARTT de l'uB, mis à jour au 9 décembre 2008 comprenant l'Organisation des services et Aménagement du Temps de Travail à l'uB ; la circulaire du ministère en date du 21 janvier 2003 sur la mise en œuvre de l'ARTT et la récupération des congés non pris du fait de l'intervention de congés pour raisons de santé ou autres ; la note du Président de l'uB du 25 septembre 2012 ayant pour objet la circulaire ministérielle du 30 avril 2012 sont applicables. Elles sont explicitées en **annexe 1**.

Pour le personnel CNRS :

L'agent permanent travaillant selon une durée hebdomadaire de travail de 38h30 *(mentionnée à l'article 3.1 du présent règlement intérieur)* bénéficie de :

- 32 jours ouvrés de congés annuels (du lundi au vendredi) par année civile (1er janvier au 31 décembre) ;
- 12 jours au titre de l'Aménagement et de la Réduction du Temps de Travail (jours RTT), (en application de l'article 8 du cadrage national du CNRS, déduction faite de la journée de solidarité ;
- 1 à 2 jours de congés accordés au titre du fractionnement (1 jour quand les congés sont pris en dehors de la période du 1er mai au 31 octobre pour une durée de 5 à 7 jours et 2 jours si cette durée est au moins égal à 8 jours).

L'agent non-permanent travaillant selon une durée hebdomadaire de travail de 36h11 *(mentionnée à l'article 3.1 du présent règlement intérieur)* bénéficie de :

- 32 jours ouvrés de congés annuels (du lundi au vendredi) par année civile (1er janvier au 31 décembre) ;
- 1 à 2 jours de congés accordés au titre du fractionnement (1 jour quand les congés sont pris en dehors de la période du 1er mai au 31 octobre pour une durée de 5 à 7 jours et 2 jours si cette durée est au moins égal à 8 jours).
- Ou
- 2.5 jours ouvrés de congés annuels (du lundi au vendredi) par mois, pour les contrats à courtes durées inférieurs à 12 mois.

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 (selon les Décisions du Président de l'uB, du Directeur de l'UFR SVTE, et du Délégué Régional de la Délégation CNRS Centre Est). 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 uB :

L'agent permanent et non permanent travaillant selon une durée hebdomadaire de travail de 37h30 et dont l'engagement est d'une durée supérieur à 10 mois *(mentionnée à l'article 3.1 du présent règlement intérieur)* bénéficie de :

- 49 jours ouvrés de congés annuels (du lundi au vendredi) par année universitaire (1er septembre de l'année N au 31 août de l'année N+1) ;
  (en application du guide ARTT de l'uB) ;

- 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).

Ou

- 2.5 jours ouvrés de congés annuels (du lundi au vendredi) par mois, pour les contrats à courtes durées inférieurs à 12 mois.

4.2. Conditions d'octroi et d'utilisation

4.2.1 Conditions d'octroi

Personnels relevant du CNRS : l'octroi des congés fait nécessairement l'objet d'une demande préalable auprès du responsable d'équipe ou du Directeur d'unité par l'application Web AGATE. Un délai de prévenance de 7 jours calendaires ou 5 jours ouvrés (du lundi au vendredi) doit être respecté.

Personnels relevant de l'uB : l'octroi des congés fait nécessairement l'objet d'une demande préalable auprès du responsable d'équipe ou du Directeur d'unité puis transmise gestionnaire RH de l'UFR et au Responsable Administratif de l'UFR SVTE. Un délai de prévenance de 7 jours doit être respecté.

Les congés sont accordés sous réserve des nécessités du service.

4.2.2 Conditions d'utilisation

Personnels relevant du CNRS :
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].

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. Le suivi des congés (annuels et RTT) est réalisé dans l'Unité sous la responsabilité du Directeur de l'Unité par l'application Web AGATE.

Personnels relevant de l'uB :
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].

Le report des jours de congés annuels et des jours RTT non utilisés pendant l'année universitaire est autorisé jusqu'au 31 décembre de l'année civile de référence. Pour les personnels BIATSS : 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 par le Pôle RH/BIATSS.

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 :

Personnels relevant du CNRS :en application de l'article 8 du cadrage national du CNRS, déduction d'une journée sur le nombre total de RTT initial*(mentionnée à l'article 4.1 du présent règlement intérieur)*;

Personnels relevant de l'uB : en application au guide ARTT, les personnels sont tenus de déposer une journée de congé/RTT ; ou bien de travailler une journée supplémentaire porte ouverte ou heures supplémentaires (en application du guide ARTT de l'uB).

4.4. Compte épargne temps (CET)

Pour le personnel CNRS :

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.

Le CET peut être alimenté soit par l'application Web AGATE ou à l'aide du formulaire spécifique disponible sur le site internet du CNRS lors de la première ouverture et alimentation. Cette demande d'alimentation matérialisée doit être accompagnée d'un décompte précis des congés pris par l'agent et d'une attestation signée du Directeur de l'Unité.
L'alimentation du CET s'effectue au plus tôt le 1er novembre et au plus tard le 31 décembre de l'année.
Le choix d'options du CET doit s'effectuer au plus tard le 31 janvier de l'année N+1.

La gestion et le suivi du CET sont confiés au service des ressources humaines de la délégation régionale du CNRS et à l'application web AGATE.

Personnels relevant de l'uB :

En application au guide ARTT, à la note d'information du Pôle RH/BIATSS, les personnes sont tenues de se rapprocher du gestionnaire RH de l'UFR et du Responsable Administratif de l'UFR SVTE.

Article 5 : Absences

5.1. 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 qui doit être transmis au service RH de son employeur.

5.2 Autorisation d'absences et aménagement d'horaires

(cf. annexe n° 1)

Article 6 : 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.

Pour les personnels uB et des autres organismes l'ordre de mission à l'étranger ou Dom-Tom, doit être signé par le Président de l'uB ou l'employeur du missionnaire. La règlementation impose l'autorisation préalable du fonctionnaire sécurité défense pour les missions des agents CNRS et uB dans certains pays étrangers à risques.

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. Une copie d'assurance du véhicule personnel de l'agent en cours de validité doit être transmise au service gestion.

Chapitre 3 : Santé et sécurité au travail

Article 7 : Personnes ressources en matière de sécurité et de prévention des risques

7.1 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.

7.2 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 **(cf. annexe 3)**
Deux assistants de prévention ont été nommés :

- M. Ludovic Bruneau (3e étage aile sud, bureau 320, tél. 6378) en charge de la sécurité des activités au 3e étage aile sud et corps central sud ainsi que le rez-de-jardin corps central
- Mme Maria Teixeira Brandao (3e étage corps central nord, bureau 321, tél. 6384) en charge de la sécurité des activités au 4é étage aile sud, au 3e étage aile nord et corps central nord ainsi que les animaleries situées au rez-de-jardin

7.3 Equipiers de sécurité Incendie

Des serre-files (chargés d'évacuation) ont été nommés afin de couvrir l'ensemble des locaux du laboratoire :

- M. Dominique Champagnac (rez-de-jardin corps central nord & animaleries, atelier, tél. 6375)
- M. Pascal Taubaty (rez-de-jardin corps central sud, atelier litholamellage & animalerie, tél. 6365)
- M. Jean Emmanuel Rollin (3e étage aile nord, bureau 311C, tél. 3946)
- M. FX Dechaume-Montcharmont (3e étage aile nord, bureau 317, tél. 9031)
- M. Frédéric Marin (3e étage corps central nord, bureau 302, tél. 6372)
- Mme Maria Teixeira Brandao (3e étage corps central nord, bureau 321, tél. 6384)
- M. Emmanuel Fara (3e étage corps central sud, bureau 314, tél. 3970)
- M. Rémi Laffont (3e étage corps central sud, bureau 313, tél. 6373)

- M. Ludovic Bruneau (3e étage aile sud, bureau 320, tél. 6378)
- M. Alain Festeau (3e étage aile sud, bureau 307, tél. 6353)
- M. Julien Pergaud (4e étage aile sud, tél 3822)
- Benjamin Pohl (4e étage aile sud, tél 3821)

7.4 Personnes compétentes en radioprotection

En raison de la présence d'équipements générateurs électriques de rayons X, des personnes compétentes en radioprotection ont été nommées:

- M. Ludovic Bruneau (3e étage aile sud, bureau 320, tél. 6378)
- M. Rémi Laffont (3e étage corps central sud, bureau 313, tél. 6373)

7.5 Membres de l'instance de concertation

L'Unité ne disposant ni de CHSCT commun aux tutelles ni d'une instance de concertation, les assistants de prévention sont conviés une fois par an au conseil d'Unité afin de présenter un bilan des actions passées dans le domaine Hygiène et Sécurité.

Les CHSCT 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 dans :

- l'arrêté CHSCT/1/2012 pour l'uB
  http://intranet.u-bourgogne.fr/upload/site_2/hygiene_securite_environnement/acteurs/chsct/arrete_siege_par_syndicat_2012.pdf
- la décision n° DEC121971DR06 du 3 juillet 2012
  https://extranet.dr6.cnrs.fr/Prevention/IMG/File/CHSCT/representativite_CRHSCT_2012.pdf

Article 8 – Organisation de la prévention au sein de l'Unité

8.1 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).

Le Directeur doit veiller à ce que chaque agent de son Unité se présente aux convocations du service de médecine de prévention.

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

Le recensement des locaux à risques, la description de la nature des risques ainsi que les mesures de prévention mises en place ont été consignés dans le document unique du laboratoire (cf. http://biogeosciences.u-bourgogne.fr/fr/component/content/article/38-fr/umr-pratique/umr-pratique/219-le-laboratoire-en-pratique#hygiene). Ce document est actualisé une fois par an avec l'aide des personnels responsables des services.

L'utilisation des véhicules du laboratoire est soumise à une autorisation préalable à la première utilisation (par la signature de la charte d'utilisation des véhicules). Cette charte peut être trouvée avec les pochettes des véhicules et doit être signée et déposée auprès du service Gestion / Administration du laboratoire.

Lors de l'arrivée de nouveaux personnels, les assistants de prévention transmettent la fiche « accueil des nouveaux entrants » au service Hygiène et Sécurité de l'université et au Médecin de Prévention afin d'identifier les risques potentiels auxquels ils seront exposés. Concernant le risque chimique, une fiche individuelle d'exposition est établie chaque année pour tout personnel concerné et transmise au service Hygiène et Sécurité de l'université et au Médecin de Prévention.

La nature des locaux à risques ainsi que leur conditions d'accès et d'utilisation sont précisées dans le tableau suivant :

Service	Responsable(s)	Horaires d'ouverture	Consignes spécifiques*
GISMO et Salle de Broyage	J. Lévêque L. Bruneau T. Cocquerez	8h30-12h/13h30-17h30	Cf. règlement de la plateforme GISMO Cf. consignes spécifiques à la DRX
Salles de préparation Pal & Bio	E. Steimetz	8h30-12h/13h30-17h30	Cf. consignes spécifiques du service
MorphOptics	R. Laffont N. Navarro P.Y. Collin	8h30/18h00	Cf. consignes spécifiques du service Cf. consignes spécifiques au µCT scan
Biologie, Génétique, Biominéralisation	M. Teixeira Brandao	8h30/18h00	Cf. consignes spécifiques du service Cf. consignes spécifiques de la salle de bactériologie
Animaleries	S. Motreuil	8h30/18h00	Cf. consignes spécifiques du service Astreintes : tour de garde d'un personnel animalier durant les week-ends, vacances scolaires et jours fériés. Possibilité de travail isolé
Service des collections	J. Thomas	9h00/18h30	Cf. consignes spécifiques du service
Salle des roches	E. Steimetz	8h30-12h/13h30-17h30	Cf. consignes spécifiques du service

*les consignes spécifiques peuvent être trouvées auprès des responsables et doivent être consultées (et éventuellement signées) avant d'utiliser le service pour la première fois.

8.3 Organisation des secours

Selon les consignes de l'université de Bourgogne : cf. plan de prévention incendie. Il est rappelé l'obligation pour tout le personnel de participer aux exercices d'évacuation organisés par l'université. Un plan d'intervention en cas d'urgence a été établi pour l'unité (**cf. annexe n°2** plan d'urgence). Les numéros d'appel et les consignes générales d'urgence sont indiqués dans le document **annexe n°2**.

Numéros des urgences spécifiques :

- Centre antipoison 03 83 22 50 50
- SOS main03 80 55 55 55

Des Sauveteurs Secouristes du Travail ont été formés :

- M. Sébastien Motreuil (3e étage aile nord, bureau 321, tél. 9198)
- Mme Maria Teixeira Brandao (3e étage corps central nord, bureau 321, tél. 6384)

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

Rayonnement ionisant : les consignes spécifiques sont données en **annexe n°2**.

Agent chimique dangereux : les consignes en cas de déversement sont données à l'adresse Web suivante :
http://intranet.u-bourgogne.fr/upload/site_2/hygiene_securite_environnement/demarche_et_instruments/procedure_deversementvalide_chs.pdf

8.5 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.

8.6 Formation à la sécurité

Le Directeur de l'Unité doit s'assurer que les agents placés sous son autorité, notamment les nouveaux entrants, ont bien reçu une formation à la sécurité et, le cas échéant, une formation spécifique adaptée à leur poste de travail. Il doit en garantir la traçabilité.

Formation des nouveaux entrants : chaque nouvel entrant devra suivre une formation courte par l'un des assistants de prévention sur la politique de sécurité du laboratoire.

Autres formations : elles sont définies en concertation avec l'assistant de prévention. Les formations à la sécurité devront être intégrées au plan de formation de l'Unité.

8.7 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 se situe dans le bureau 321 du corps central nord.

Un registre de signalement de danger grave et imminent, ouvert au timbre du CHSCT compétent, doit être mis à la disposition des agents : le Directeur d'Unité doit porter à la connaissance des agents l'emplacement de ce registre dans l'établissement, et s'il y a lieu, en mettre un à disposition.

8.8 Accueil de personnes extérieures

Stagiaires et visiteurs :

L'accueil de stagiaires et de visiteurs doit être organisé et encadré :

- convention de stage pour les stagiaires ;
- déclaration de visite auprès du Service Gestion / Administration pour les visiteurs ;
- déclaration via l'application CNRS - ASSET pour les visiteurs étrangers (hors UE) et auprès du RSSI de l'uB.

Entreprises extérieures :

Lors de l'intervention d'entreprises extérieures dans l'Unité, une visite de prévention et, s'il y a lieu, un plan de prévention doit être réalisé.

8.9 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 (voir paragraphe 1.6).

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 4)***.
Indiquer l'organisation proposée au sein du service ou au poste de travail.

Article 9 – Interdictions

9.1 Animaux domestiques

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

9.2 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.

9.3 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 10 : Confidentialité, publications et communication, propriété intellectuelle

10.1 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 éléments 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 de l'Unité et sont détaillées par la PSSI opérationnelle de l'Unité.

10.2 Publications et communication

10.2.1 Autorisation préalable du Directeur de l'Unité

Nonobstant les dispositions de l'article 10.1, les personnels de l'Unité peuvent, après autorisation du Directeur de l'Unité et du responsable scientifique du projet le cas échéant et en accord 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 applicable lorsque le sujet de la publication relève d'un secteur protégé,
- les droits d'auteurs sur les textes, images, sons, vidéos...

10.2.2 Formalisme des publications et communication

Les publications (de toute nature) des personnels de l'Unité font apparaître le laboratoire et le lien avec les organismes de tutelle dans une « signature commune » à tous les membres du laboratoire. Dans le cas d'un chercheur dont l'employeur n'est pas tutelle de l'UMR, cet employeur est ajouté à la signature commune. L'appartenance à une équipe interne peut être ajoutée (de préférence dans les remerciements), mais ne doit en aucun cas se substituer à la « signature commune ». Le complément d'adresse postale (6 boulevard Gabriel) peut être associée à l'auteur auquel la correspondance est adressée.

Signatures communes des travaux issus du laboratoire :

1. Cas d'une signature multiligne :

nom et prénom de(s) l'auteur(s) ;
1. Biogéosciences UMR6282, Univ. Bourgogne Franche-Comté, F-21000 Dijon, France ;
2. Biogéosciences UMR6282, CNRS, F-21000 Dijon, France ;

2. Cas d'une signature monoligne :

nom et prénom de(s) l'auteur(s) ;
Biogéosciences UMR6282, CNRS, Univ. Bourgogne Franche-Comté, F-21000 Dijon, France

L'ensemble des publications (articles, chapitres, ouvrages, actes, …) dont tout ou partie du travail a été effectué à l'Unité doit faire l'objet d'un signalement dès parution à Rémi Laffont avec les informations nécessaires à l'identification de ces publications (titre, auteurs, pagination,…). Dans la mesure du possible, un exemplaire électronique (pdf) des articles doit également être remis à Rémi Laffont.

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.

Pour les seuls secteurs scientifiques sensibles : toute communication, enseignement, qu'il s'agisse d'un colloque, d'un séminaire ou d'un congrès est soumise à autorisation du Haut Fonctionnaire Sécurité Défense du MESR par l'intermédiaire du Fonctionnaire sécurité Défense du CNRS.

10.2.3 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.

10.2.4 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.

10.3 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).

10.4 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.

10.5 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 11 : 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 l'uB, les sanctions disciplinaires sont prises en application des règles régissant chaque corps de personnels.

Article 12 : Formation

12.1 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 régionale du CNRS du suivi des agents.

Le plan de formation est transmis au service des ressources humaines de la Délégation régionale du CNRS ainsi qu'au service formation de l'autre (ou autres tutelles) de l'unité, service formation qui peut aussi financer des actions de formation pour les personnels du laboratoire.

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.

12.2 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 13 : Utilisation des moyens informatiques et Sécurité des systèmes d'information

L'utilisation des moyens informatiques de l'Unité est soumise aux dispositions de la Charte Sécurité des Systèmes d'Information en vigueur dans l'Unité (Charte SSI du CNRS ou du partenaire).

Cette Charte, qui a notamment pour objet de préciser la responsabilité des utilisateurs au regard de la législation, doit être signée par tout nouvel arrivant.

La Charte Sécurité des Systèmes d'Information figure en **annexe n°5** du présent règlement intérieur.

L'utilisation des moyens informatiques de l'Unité est par ailleurs soumise à des règles de sécurité qui sont détaillées dans la PSSI opérationnelle de l'Unité, cohérente avec le dispositif de protection du potentiel scientifique et technique, également annexée au présent règlement intérieur **(cf. annexe n° 6)**.

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

Article 14 : Utilisation des ressources techniques collectives

Les ressources techniques collectives sont organisées en « services » et « plateformes ». Leur liste est disponible sur l'organigramme du laboratoire (cf. site Web pour trouver cet organigramme).

Chaque utilisateur de ces ressources collectives doit se référer aux règles spécifiques en vigueur au sein de ces « services » et « plateformes ».

Article 15 : 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 16 : Publicité

Le présent règlement intérieur est porté à la connaissance des agents par voie d'affichage dans les locaux de l'Unité. Il annule et remplace le règlement intérieur du 01 janvier 2005 et entre en vigueur au 09/09/2015

Il est ensuite consultable au service Gestion / Administration du laboratoire.

Fait à Dijon, le 09 aout 2015

Signature des représentants légaux des tutelles

Visa du Directeur de l'Unité

ANNEXE N°1 : AUTORISATION D'ABSENCES ET AMENAGEMENT D'HORAIRES

/

ANNEXE N°2 : CONSIGNES D'URGENCE

Délégation Centre Est

Informations pour intervention en cas d'urgence dans l'unité 6282.

UNIVERSITÉ DE BOURGOGNE

Personnes à contacter au sein de l'Université

Président de l'Université Mr BONNIN Alain

Tel bureau :03 80.29.36.03 Fax : 03 80.29.32.80 Email : : Alain.Bonnin@u-bourgogne.fr

Directeur General des Service: M. ROBIN Gilles
Tel bureau :03 80.39.55.13 Fax : 03 80.39.50.69 Email : : gilles.robin@u-bourgogne.fr

Ingénieur hygiène et sécurité Mme BOUCHOT Pascale

Tel bureau : 03 80.39.55.45 Tel portable : 06 80.88.73.49 Fax : 03 80.39.55.44
Email : pascale.bouchot@u-bourgogne.fr

Directeur du Service Technique de l'Université M SICCARDI Etienne

Tel de permanence : 03.80.39.50.70 Tel portable de permanence : 06 85.42.81.52 Fax : 03.80.39.89.96

Email : etienne.siccardi@u-bourgogne.fr

Personnes à contacter au sein de la formation de recherche

Directeur de la structure : Mr NEIGE Pascal (Directeur de l'UMR)

Tel bureau : 03 80 39 63 57 Tel portable : 06 18 62 75 32

Correspondant hygiène et sécurité : Mme TEIXEIRA Maria

Tel bureau 03 80 39 63 78 Tel portable : Tel domicile :

Personne compétente en radioprotection :

1. Mr BRUNEAU Ludovic

Tel bureau 03 80 39 63 78 Tel portable : 06 74 22 56 73

2. Mr LAFFONT Rémi

Tel bureau 03 80 39 63 73 Tel portable : 06 18 93 73 94

Délégation Centre Est

Informations pour intervention en cas d'urgence dans l'unité 6282.

UNIVERSITE DE BOURGOGNE

Caractéristiques techniques générales de la formation de recherche

Structure

Intitulé de la structure : UMR CNRS 6282 BIOGEOSCIENCES
Localisation (bâtiment, aile etc..) : Bâtiment de Gabriel – 6 boulevard de Gabriel – 21000 Dijon

Coupure alimentation électrique	Oui ■ Non☐	Lieu : Loge Gabriel
Coupure générale d'eau	Oui ■ Non☐	Lieu d'implantation de la coupure : sous-sol
Installation générale de vide	Oui ☐ Non ■	Lieu d'implantation de la coupure :
Alimentation en gaz de ville	Oui ☐ Non ■	Lieu d'implantation de la coupure :
Bonbonnes ou cartouches de gaz (butane, propane)	Oui ☐ Non ■	Lieu d'implantation ou de stockage :

Bouteilles de gaz comprimés : Air, $CO_{2,}$, , …

Précisez :

■ $CO_{2,}$	Lieu d'implantation ou de stockage : 310 S,309 S et 1P (3ème étage)
■ N_2	Lieu d'implantation ou de stockage : 310 S,309 S et 1P (3ème étage)
■ N_2 liquide	Lieu d'implantation ou de stockage : 310 S et 309 S
■ CO	Lieu d'implantation ou de stockage : 310 S
■ Hélium	Lieu d'implantation ou de stockage : 310 S et 309 S
■ CH4	Lieu d'implantation ou de stockage : 310 S et 309 S
■ Acétylène	Lieu d'implantation ou de stockage : -
■ Argon	Lieu d'implantation ou de stockage : 310 S et 309 S
■ Protoxyde d'azote	Lieu d'implantation ou de stockage : 310 S et 309 S

Locaux à accès restreint (badge, code etc..)

Pièce(s) N° : Corp central : 307, D, E, F, G, H
Aile Sud : 309 à 317 et palier sud 3 C
Aile Nord 322, 321, 320, 310, Palier nord 1 P, 2P, 3P, 4P
Clef Ecologie, biomin ou Géologie (SEDS labo)

N : Aile Nord S : Aile Sud C : Corps Central P : Palier

Délégation Centre Est

Informations pour intervention en cas d'urgence dans l'unité 6282.

UNIVERSITÉ DE BOURGOGNE

Identification des locaux à risques

Risque biologique

Laboratoire de confinement L2	Oui ☐ Non ■	Lieu d'implantation :
Laboratoire de confinement L3	Oui ☐ Non ■	Lieu d'implantation :
Animalerie	Oui ■ Non ☐	Lieu d'implantation : Autre unité : Animalerie Ss aile nord
Stockage des déchets biologiques	Oui ■ Non ☐	Lieu d'implantation : Ss aile nord Autre unité

Risque chimique

Manipulation de produits C.M.R. (Cancérogènes, Mutagènes, Toxiques pour la reproduction)	Oui ■ Non ☐	Lieu d'implantation : 301B N, palier nord 1P à 4P, 315 S et 317 S
Présence de produits inflammables	Oui ■ Non ☐	Lieu d'implantation : 324 C 315 S et 317 S
Présence de produits psychotropes	Oui ☐ Non ■	Lieu d'implantation :
Présence de drogues ou de leurs précurseurs	Oui ☐ Non ■	Lieu d'implantation :
Armoires de stockage	Oui ■ Non ☐	Lieu d'implantation : 302 C et 316 S
Stockage des déchets chimiques	Oui ■ Non ☐	Lieu d'implantation : Soute extérieur

Risque radioactif

Sources non scellées

Liste des radioéléments détenus :		Lieu d'utilisation :	
Autres autorisation :	T210203	aile nord RDC	PCR : Sandrine Bellenger
	T210210	aile nord 2ème étage	PCR : Stéphane Fraichard
	T210287	corps central 2ème étage	PCR : Catherine Gondcaille

Sources scellées

Irradiateur	Oui ☐ Non ■	Lieu d'implantation :
Compteurs à scintillation	Oui ☐ Non ■	Lieu d'implantation :
Zone contrôlée	Oui ☐ Non ■	Lieu d'implantation :
Zone(s) surveillée(s)	Oui ■ Non ☐	Lieu d'implantation : enceinte de l'appareil salle 311 S et 307E C
Stockage des déchets radioactifs	Oui ■ Non ☐	Lieu d'implantation : S04C Pour les autres autorisations

N : AileNnord S : Aile Sud C : Corps Central

Juin 2014 4

BIOGÉOSCIENCES

Consignes de sécurité

Personnes à prévenir en cas d'incident radiologique

Rémi LAFFONT **Ludovic BRUNEAU** *Personnes Compétentes en Radioprotection* **Téls : 03 80 39 63 73 / 03 80 39 63 78**	**Anne CARRERE** *Médecin du travail* **Tél : 03-80-39-51-61**
C DURLET / JF DECONINCK / N NAVARRO *Resp. du pistolet XRF / DRX / µCT scan* **Tél : 03 80 39 + 39 73 / 63 31 / 63 61**	**Pascal NEIGE** *Directeur de l'UMR 6282 Biogéosciences* **Tél : 03 80 39 63 57**

Autorités à prévenir en cas d'incident radiologique

Autorité de Sûreté Nucléaire *Direction des Transport et des Sources* **15-21, rue Louis-Lejeune** **CS 70013** **92120 Montrouge** **Tel : 01 46 16 40 00** **Fax : -**	**Autorité de Sûreté Nucléaire** *Division de Dijon* **21 boulevard voltaire** **BP 37815** **21078 Dijon Cedex** **Tél : 03 45 83 22 66** **Fax : 03 45 83 22 94**
Préfecture de la Région Bourgogne et de la Côte d'Or **53, rue de la préfecture** **21041 DIJON cedex** **Tel : 03 80 44 64 00** **Fax : 03 80 30 65 72**	**Institut de Radioprotection et de Sûreté Nucléaire** **31, avenue de la Division Leclerc** **92260 Fontenay-aux-Roses** **Tél : 01 58 35 88 88** **Fax : 01 58 35 84 51**

Numéro Vert ASN (situation d'urgence et incident radiologique) :

0800 804 135

UMR CNRS 6282 Biogéosciences – Université de Bourgogne

6, Boulevard Gabriel – 21000 DIJON

BIOGÉOSCIENCES

Consignes de sécurité

L'accès à ce local est réservé au personnel concerné et formé aux risques radiologiques

Toute personne entrant dans ce local doit être clairement informée de la **présence d'un générateur à rayons X**, des risques associés, ainsi que la signification des signalisations.

Pour les besoins de formations des étudiants, une **Autorisation Exceptionnelle** peut être accordée à l'enseignant-chercheur qui en fait la demande : Contacter la Personne Compétente en Radioprotection (Poste 63 78).

Description des risques

Exposition externe, partielle ou globale au rayonnement ionisant.

Pour le risque d'incendie ou dégâts des eaux, se conformer aux consignes de sécurité générales

Conditions d'utilisation

Mise en route de l'appareil obligatoirement par une personne autorisée
Respecter scrupuleusement la procédure de mise sous tension de l'appareil, ainsi que les conditions d'utilisation.

Conduite à tenir en cas d'accident

Supprimer les rayonnements à la source en mettant le générateur hors tension.
S'éloigner du lieu de l'accident en sortant de la salle.
Interdire l'accès de la zone en refermant la salle à clé.
Prévenir la Personne Compétente en Radioprotection (poste 63 78) ainsi que le médecin du travail (poste 51 61).

UMR CNRS 6282 Biogéosciences – Université de Bourgogne
6, Boulevard Gabriel – 21000 DIJON

CONSIGNES GENERALES D'URGENCE

Protocole d'appel en cas de PROBLEMES TECHNIQUES

Quelque soit l'heure, vous appelez les Services techniques au 50 70

En cas de non réponse,

Composez le 76 76 en interne ou le 06 85 42 81 52 d'un portable

Indiquez clairement :

- ***Votre nom et le nom du laboratoire***
- ***Le n° de téléphone d'où vous appelez***
- ***Le lieu exact de l'incident (bâtiment, aile, étage, salle)***
- ***La nature du sinistre (effraction, fuite, problème électrique),***
- ***Les premières mesures prises***

INTRUSION/AGRESSION :

En cas d'urgence appelez ou faites appelez les forces de police au 75 45 de tout poste de l'université ou le 17 d'un portable.

Organisation de secours :
Donnez l'adresse suivante

Batiment Gabriel
6 Boulevard Gabriel 21000 DIJON

Protocole d'APPEL en cas d'URGENCE MEDICALE

1° APPELEZ le 75 06 (De tous postes téléphoniques de l'Université)
Ou le 03 80 66 14 68 de votre portable

2° INDIQUEZ de façon claire et précise :

- ***Votre nom et prénom et le nom du laboratoire***
- ***Le n° de téléphone d'où vous appelez***
- ***Le lieu exact de l'incident (bâtiment, aile, étage, salle)***
- ***Le nombre de blessés***
- ***L'état de la victime (est-elle consciente ? respire-t-elle ? a-t-elle des douleurs ? saigne-t-elle ?...)***

3° PREVENEZ ensuite la personne à la loge/à l'accueil du bâtiment.
4° ENVOYEZ quelqu'un pour accueillir et diriger les secours.

Attitude à tenir en cas d'INCENDIE

Garder son calme
Attaquer le feu avec l'extincteur approprié le plus proche
Si les flammes ne peuvent être maîtrisées, percuter le bouton du boîtier alarme-incendie
Prévenez l'agent de la loge au 50 03 et donnez toutes les informations utiles
En cas d'absence, téléphoner aux pompiers 7544
Préciser clairement

- ***Le lieu du sinistre (rue, bâtiment, aile, étage, salle)***
- ***La nature du problème***
- ***Le nombre de blessés***
- ***Les premières mesures prises***

Tout retour en arrière doit être empêché. L'ascenseur ne doit pas être emprunté

ANNEXE N°3 : 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° 4 : 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°5 : CHARTE SUR LA SECURITE DES SYSTEMES D'INFORMATION

Charte d'usage des technologies de l'information et de la communication

à l'Université de Bourgogne

Votée par le conseil d'administration de l'université de Bourgogne le 28 juin 2007. Cette charte vaut pour règlement intérieur en ce qui concerne l'usage des TIC .

Préambule

Le *système d'information* est constitué de l'ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications, pouvant être mis à la disposition de l'*utilisateur*.

L'informatique nomade, constituée par les assistants personnels, les ordinateurs portables, les téléphones portables, …, est également un des éléments constitutifs du système d'information.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent et notamment, la sécurité, la performance des traitements et la conservation des données personnelles.

La présente charte définit les règles d'usage et de sécurité que l'institution et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun.

La charte est accompagnée d'une **annexe juridique** qui rappelle les dispositions législatives en vigueur pour son application. Elle pourra être complétée par un **guide d'utilisation** définissant les principales pratiques d'usage.

L'Université de Bourgogne porte à la connaissance de l'utilisateur la présente charte.

Engagements de l'institution

L'Université de Bourgogne s'engage à mettre en œuvre les moyens nécessaires destinés à assurer la sécurité du système d'information et la protection des utilisateurs.
Elle facilite l'accès des utilisateurs aux ressources du système d'information qui sont dédiées à l'enseignement, à la recherche, à la documentation et à la gestion de l'Université.
Les ressources mises à disposition sont prioritairement à usage universitaire, mais l'institution est tenue de respecter la vie privée de chacun.

Engagement de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique et de déontologie.

Les utilisateurs ont une responsabilité particulière dans l'utilisation qu'ils font des ressources mises à leur disposition par l'Université.
En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

Article I . Champ d'application

Un utilisateur est une personne physique (étudiant, enseignant, chercheur, ingénieur, technicien, administratif, personnel de service, personnel temporaire, stagiaire, ...) autorisée à accéder à l'une des ressources du système d'information.

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'institution ainsi qu'à l'ensemble des utilisateurs.

Les utilisateurs ayant des fonctions d'administrateur de systèmes d'information sont soumis à une charte complémentaire et spécifique précisant leurs obligations particulières.

Article II . Conditions d'utilisation des systèmes d'information

Section II.1 Utilisation universitaire privée

Les systèmes d'information universitaires sont mis à disposition de l'utilisateur.

L'utilisation à des fins privées doit être non lucrative et raisonnable, tant dans la fréquence que dans la durée. Elle ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

Toute information est réputée universitaire, à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace prévu explicitement à cet effet, dont la sauvegarde lui incombera.

Section II.2 Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer cette continuité, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux systèmes d'information.

L'utilisateur est responsable de son espace de données à caractère privé qu'il doit détruire lors de son départ définitif. Les mesures de conservation professionnelles sont définies avec le responsable désigné au sein de l'institution.

Article III . Principes de sécurité

Section III.1 Règles de sécurité applicables

L'institution met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs.
Les utilisateurs sont informés que les mots de passe constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas un caractère personnel aux outils informatiques protégés.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée . La sécurité des systèmes d'information mis à sa disposition lui impose :

- De respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe ;
- De garder strictement confidentiels son (ou ses) mot(s) de passe et de ne pas le(s) dévoiler à un tiers ;
- De respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre utilisateur, ni chercher à les connaître

Par ailleurs, la sécurité des ressources mises à la disposition des utilisateurs nécessite plusieurs précautions :

➢ De la part de l'institution :

- Veiller à ce que les ressources sensibles ne soient pas accessibles en cas d'absence (en dehors des mesures de continuité mises en place par la hiérarchie) ;
- Limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité

➢ De la part de l'utilisateur :

- Si l'utilisateur de bénéficie pas d'une habilitation explicite, il doit s'interdire d'accéder ou tenter d'accéder à des ressources du système d'information, même si cet accès est techniquement possible ;
- Ne pas connecter directement aux réseaux locaux des matériels non confiés ou non autorisés par l'institution [ ]
- Ne pas installer, télécharger ou utiliser sur le matériel de l'institution, de logiciels ou progiciels sans autorisation explicite ;
- Se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques ;

Section III.2 Devoir de signalement et d'information

L'institution doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information.

L'utilisateur doit avertir sa hiérarchie dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, etc. : il signale également à la personne responsable du site toute possibilité d'accès à une ressource qui ne corresponde pas à son habilitation.

Section III.3 Mesures de contrôle de la sécurité

L'utilisateur est informé :

- Que pour effectuer la maintenance corrective, curative ou évolutive, l'institution se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- Qu'une maintenance à distance est précédée d'une information de l'utilisateur ;
- Que toute information bloquante ou présentant une difficulté technique d'acheminement à son destinataire, peut être isolée, le cas échéant supprimé.

L'institution informe l'utilisateur que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Article IV . Communications électroniques

Section IV.1 Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail et de mutualisation de l'information au sein de l'institution.

La messagerie est un outil de travail ouvert à des usages professionnels et pédagogiques : elle peut constituer le support d'une communication privée (usage restreint).

Des règles précises réglementent l'utilisation de la messagerie électronique pour :

a) l'attribution des adresses électroniques

b) le contenu des messages électroniques

c) l'émission et la réception des messages

d) le statut et la valeur juridique des messages

e) le stockage et l'archivage des messages

(cf guide d'utilisation en annexe)

Section IV.2 Internet

Il est rappelé que le réseau Internet est soumis à l'ensemble des règles de droit en vigueur.

L'utilisation de la technologie Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'institution.

L'institution met un accès Internet à disposition de l'utilisateur chaque fois que cela est possible.

Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogique) : il peut constituer le support d'une communication privée dans le respect de la législation en vigueur. En complément de ces dispositions légales et au regard de la mission éducative de l'institution, la consultation volontaire et répétée de contenus à caractère pornographique depuis les locaux de l'institution est proscrite.

L'institution se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle à priori ou à posteriori des sites visités et des durées d'accès correspondantes.

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'institution.

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formations ou de sensibilisation.

Section IV.3 Téléchargements

Sur le réseau Internet, tout téléchargement de fichiers, notamment de sons ou d'images, doit s'effectuer dans le respect des droits de la propriété intellectuelle.

L'institution se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information, code malicieux, programmes espions …)

Article V. Traçabilité

L'institution est dans l'obligation légale de mettre en place un système de journalisation* des accès Internet, de la messagerie et des données échangées.

**conservation des informations techniques de connexions telles que l'heure d'accès, l'adresse IP de l'utilisateur…*

L'institution se réserve le droit de mettre en place des outils de traçabilité sur tous les systèmes d'information, après avoir procédé à une déclaration auprès de la CNIL (Commission Nationale de l'informatique et des Libertés) mentionnant notamment la durée de conservation des traces et durées de connexions.

Article VI. Respect de la propriété intellectuelle

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

En conséquence, chaque utilisateur doit :

- utiliser les logiciels dans les conditions souscrites ;

- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protéges par le droit d'auteur ou un droit privatif, sans voir obtenu préalablement l'autorisation des titulaires de ces droits.

Article VII. Respect de la loi informatique et libertés

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n°78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée par la loi n°2004-801 du 6 août 2004.

Article VIII. Limitation des usages

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation, la « personne juridiquement responsable » pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des utilisateurs, limiter les usages par mesure conservatoire.

Par « personne juridiquement responsable », on entend : toute personne ayant la responsabilité de représenter l'Université, en l'occurrence son Président et ses délégataires.

Tout abus à des fins extra-universitaires, dans l'utilisation des ressources mises à disposition de l'utilisateur, est passible de sanctions.

Article IX. Entrée en vigueur de la charte

La présente charte a valeur de règlement intérieur pour ce qui concerne l'usage des systèmes d'information.

Le présent document annule et remplace tous les autres documents ou chartes relatifs à l'utilisation des systèmes d'information.

Dijon, le 28 juin 2007

La présidente de l'Université

Sophie BÉJEAN

ANNEXE N°6 : POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION OPERATIONNELLE DE L'UNITE

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.