Règlement intérieur du
Laboratoire Magmas & Volcans

PREAMBULE

Le **Laboratoire Magmas et Volcans** (LMV) est une unité mixte de recherche implantée dans les locaux de l'Université Clermont-Auvergne (UCA), ayant également pour autres tutelles le Centre National de la Recherche Scientifique (CNRS, **UMR 6524**), l'Institut de Recherche pour le Développement (IRD, UMR 163) et l'Université Jean Monnet de Saint Etienne (UJM). C'est l'un des deux laboratoires de l'Observatoire de Physique du Globe de Clermont-Ferrand (OPGC). Le Laboratoire Magmas et Volcans (ci-après désignée l'« Unité ») est implanté sur plusieurs sites dont celui d'Aubière (63) et Saint-Etienne (42). Le règlement intérieur de l'Université Jean Monnet (**Annexe 1 - Le règlement intérieur de l'Université Jean Monnet**) s'applique sur le site de Saint-Etienne.

Le présent règlement intérieur a été soumis à l'avis du Conseil de laboratoire réuni le 19 Juin 2017.

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

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

Le présent règlement intérieur est complémentaire à celui de l'Université Clermont Auvergne pour les sites de Clermont et à celui de l'Université Jean Monnet pour le site de Saint Etienne. En cas de contradiction, les dispositions les plus restrictives prévaudront.

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

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

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

SOMMAIRE

Chapitre 1 : Fonctionnement
Article 1 : Fonctionnement général de l'Unité
1.1 Assemblée Générale
1.2 Conseil de laboratoire
1.2.1 Composition
1.2.2 Compétence
1.2.3 Fonctionnement
1.3 Autres : conseil scientifique,…
1.4 Organisation de l'Unité
1.5 Accès aux systèmes d'information (SI) de l'Unité
1.6 Accès aux locaux

Chapitre 2 : Organisation du temps de travail
Article 2 : Durée du travail

Article 3 : Horaires
3.1 Durée hebdomadaire de travail
3.2 Cycle de travail particulier (le cas échéant)
3.3 Sujétions et astreintes (le cas échéant)

Article 4 : Congés
4.1 Congés annuels et RTT
4.2 Conditions d'octroi et d'utilisation
4.2.1 Conditions d'octroi
4.2.2 Conditions d'utilisation
4.3 Journée de solidarité
4.4 Compte épargne temps (CET)

Article 5 : Absences

Article 6 : Mission

Chapitre 3 : Santé et sécurité au travail
Article 7 : Personnes ressources en matière de sécurité de santé et de prévention des risques
7.1 Directeur d'Unité
7.2 Assistant de prévention
7.3 Equipiers de sécurité incendie
7.4 Personnes compétentes dans un domaine de gestion du risque
7.5 Membres de l'instance de concertation

Article 8 : Organisation de la prévention au sein de l'Unité
8.1 Suivi médical des agents
8.2 Mesures de prévention spécifiques en fonction de l'activité et des risques
8.3 Organisation des secours
8.4 Conduite(s) à tenir en cas d'accident lié à une activité spécifique8.5 Formation à la sécurité
8.6 Registres
8.7 Accueil de personnes extérieures à l'Unité
8.8 Travail isolé
Article 9 : Interdictions
9.1 Animaux domestiques

9.2 Interdiction de fumer
9.3 Alcool

Chapitre 4 : Confidentialité, publications et communication, propriété intellectuelle
Article 10 : Confidentialité, publications et communication, propriété intellectuelle
10.1 Confidentialité
10.2 Publications et communication
10.2.1 Autorisation préalable du Directeur de l'Unité
10.2.2 Formalisme des publications et communications
10.2.3 Logos et marques
10.2.4 Création de sites web
10.3 Cahiers de laboratoire
10.4 Propriété intellectuelle
10.5 Obligation d'information du Directeur de l'Unité : Contrats, décisions de subvention et ressources propres

Chapitre 5 : Dispositions générales
Article 11 : Discipline
Article 12 : Formation
12.1 Correspondant formation
12.2 Formation par la recherche

Article 13 : Utilisation des moyens informatiques et sécurité des systèmes d'information

Article 14 : Utilisation des ressources techniques collectives

Article 15 : Durée

Article 16 : Publicité

Annexe 1 - Le règlement intérieur de l'Université Jean Monnet
Annexe 2 - Composition du conseil de laboratoire
Annexe 3 - Organigramme du LMV
Annexe 4 - Délibération du CA pour les personnels BIATSS
Annexe 5 - Autorisation exceptionnelle d'absence
Annexe 6 - Consignes de sécurité
Annexe 7 - Rôle et mission de l'assistant de prévention
Annexe 8 - Personnes ressources en matière de sécurité et de prévention des risques
Annexe 9 - Note sur le travail isolé
Annexe 10 - Charte Informatique du LMV
Annexe 11 - PSSI Opérationnelle de l'unité

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 à l'initiative du Directeur d'Unité dès qu'une question d'ordre général se pose au 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, et conformément à la décision DEC170563DR07 portant création du conseil de laboratoire, le Conseil de laboratoire de l'Unité se compose de 17 membres (**Annexe 2 - Composition du conseil de laboratoire**) :
- quatre membres de droit : le Directeur d'Unité, et les 3 directeurs-adjoints,
- quatre membres nommés : les responsables des trois équipes disciplinaires, et le responsable du site stéphanois.
- neuf membres élus : 6 dans le collège Chercheurs/enseignants chercheurs
(quatre chercheurs/enseignants-chercheurs, un chercheur sur contrat post-doctoral et un doctorant), et 3 dans le collège ITA.

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. Il est convoqué par le Directeur soit à l'initiative de celui-ci, soit à la demande du tiers de ses membres. Le conseil peut entendre, sur invitation du Directeur, toute personne participant aux travaux de l'unité, ou appelée à titre d'expert sur un point de l'ordre du jour. Le Directeur arrête l'ordre du jour de chaque séance ; celui-ci comporte toute question, relevant de la compétence du conseil de l'Unité, inscrite à l'initiative de son Directeur ou demandée par plus d'un tiers des membres de ce conseil. L'ordre du jour du conseil de laboratoire est diffusé à l'ensemble des membres du conseil au moins 8 jours à l'avance. Un relevé de décision, visé par le Directeur, est envoyé après chaque conseil.

1.3 : Autres : Conseil scientifique, comité de direction …

Le comité de direction est composé du Directeur d'Unité, des trois directeur-adjoints, des trois responsables d'équipe, des responsables d'axe transverse et de la responsable administrative.

1.4 Organisation de l'Unité

Le laboratoire comprend trois équipes disciplinaires (Géochimie, Pétrologie expérimentale et Volcanologie), épaulées par un pôle administratif et un pôle technique. (**Annexe 3 - Organigramme du LMV**). Les équipes de recherche regroupent des chercheurs, enseignants-chercheurs, doctorants et post-doctorants sous la direction d'un responsable d'équipe. Des recherches interdisciplinaires sont conduites au sein de deux axes transverses thématiques (Mécanismes géodynamiques de la Terre Primitive ; et Géologie régionale : volcanisme et environnements), chaque axe étant animé par un responsable. Le pôle administratif regroupe les secrétaires et le personnel d'entretien sous la direction de la responsable administrative. Il est en charge de la gestion financière, de la gestion administrative des personnels, de l'accueil, des bases de données (bureaux, arrivées-départs, etc.), de la formation continue et de la gestion des personnels d'entretien. Le pôle technique regroupe l'ensemble des ingénieurs, assistants-ingénieurs et techniciens travaillant dans les services communs et sur les instruments expérimentaux ou analytiques des équipes de recherche ; il est géré par le directeur technique qui définit les missions des personnels techniques en concertation avec les responsables d'équipe. *Les ressources sont affectées aux différentes équipes, axes et services, sur proposition du directeur d'unité et après validation par le conseil de laboratoire.*

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 7). 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 de l'Unité.

1.6 Accès aux locaux

La plage horaire de travail de référence (i.e., heures ouvrables du laboratoire) est :

7H30 heures à 20 heures du lundi au vendredi.

Les personnes concernées : personnels participant directement aux activités scientifiques et techniques de l'Unité (personnels permanents, stagiaires, doctorants, personnes participant à une activité de recherche et d'enseignement, en formation, effectuant une prestation de service). La possession d'un badge d'accès est obligatoire pour accéder à l'Unité.

Les nouveaux entrants en attente de badge doivent venir se présenter à l'accueil du laboratoire.

Les visiteurs doivent indiquer à la personne de l'accueil leur nom, prénom, organisme d'appartenance, ainsi que le nom de la personne visitée et le motif de la visite. Les visites se font toujours en la présence d'un personnel permanent, généralement la personne qui reçoit la visite.

• Sauf autorisation exceptionnelle délivrée par les responsables des services, sous couvert du directeur d'unité, les accès aux salles de broyage et sciage des roches, et à l'atelier de mécanique sont interdits pendant les périodes de fermeture du laboratoire (nuit, week-end, période de fermeture estivale).
• L'accès au laboratoire et l'utilisation des instruments en dehors des heures ouvrables est règlementé (cf.8.2 Mesures de prévention spécifiques en fonction de l'activité et des risques et 8.9 Travail isolé)

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

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

Chapitre 2 : Ressources humaines

Le conseil d'administration de l'Université Clermont Auvergne, en sa séance du 19 mai 2017 a voté une délibération portant organisation du temps de travail des personnels BIATSS. (**cf. Annexe 4 – Délibération du CA pour les personnels BIATSS**)

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.

Pour les personnels CNRS et IRD: la durée annuelle de travail est fixée à 1607 heures. Cette durée tient compte des 7 heures de travail dues au titre de la journée de solidarité (les modalités d'accomplissement de cette journée sont précisées à l'article 4.3 du présent règlement intérieur).
Les modalités de mise en œuvre dans l'Unité prennent en compte les dispositions du décret n°2000 - 815 du 25 août 2000 modifié et de son arrêté d'application du 31 août 2001 ainsi que celles du cadrage national du CNRS en date du 23 octobre 2001 modifié.
Pour les personnels Université : la durée annuelle de travail est fixée à 1 593 heures pour l'ensemble des personnels.

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 et IRD : l'horaire hebdomadaire est fixé à 38 heures 30 minutes

Pour les personnels Université : l'horaire hebdomadaire est fixé à :

- 37 heures 30 minutes pour l'ensemble des agents titulaires et agents non titulaires recrutés sur contrat à durée déterminée supérieure à 10 mois ;
- 35heures pour les personnels techniques et administratifs recrutés sur contrat à durée inférieure ou égale à 10 mois.

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.

Les agents bénéficient d'un repos minimum quotidien de onze heures consécutives.
Aucun temps de travail quotidien ne peut atteindre 6 heures sans que les agents bénéficient d'un temps de pause d'une durée minimale de 20 minutes non fractionnable.
Après accord du directeur d'Unité et sous condition des nécessités de service, certains personnels peuvent pratiquer un horaire décalé par rapport à la plage horaire de référence qui doit se situer entre 7 heures 30 et 20 heures.

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.

Pour le personnel CNRS et IRD : L'agent travaillant selon une durée hebdomadaire de travail de 38h30 bénéficie de : 32 jours ouvrés de congés annuels (du lundi au vendredi) par année civile (1er janvier au 31 décembre); 12 jours au titre de l'Aménagement et de la Réduction du Temps de Travail

(jours RTT) ; 1 à 2 jours de congés accordés au titre du fractionnement (1 jour quand les congés sont pris entre la période du 31 octobre au 1er mai pour une durée de 5 à 7 jours et 2 jours si cette durée est au moins égal à 8 jours).
Les agents exerçant leurs fonctions à temps partiel bénéficient d'un nombre de jours de congés annuels et de jours RTT calculés en fonction de leurs obligations hebdomadaires de service. Par exemple, un agent travaillant selon une quotité de temps de travail de 80% sur 4 jours bénéficie de 26 jours de congés annuels (32x4/5). En revanche, l'agent travaillant selon une quotité de temps de travail de 80% sur 5 jours bénéficie du même nombre de jours de congés annuels qu'un agent exerçant ses fonctions à temps plein soit 32 jours.
Les jours RTT sont, quant à eux, proratisés en fonction de la quotité de temps de travail de l'agent. Par exemple, le nombre de jours de congés annuels et RTT d'un agent exerçant ses fonctions à temps partiel selon une quotité de temps de travail de 80% sur 4 jours est calculé au prorata de la quotité travaillée. En revanche, l'agent travaillant à temps partiel selon une quotité de temps de travail de 80% sur 5 jours bénéficie du même nombre de jours de congés annuels et RTT qu'un agent exerçant ses fonctions à temps plein.

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

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

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

Pour les personnels Université :
Le nombre total de jours alloués à l'agent à temps complet est de 50 (25 jours de congés annuels au titre du décret 84-972, 20 jours au titre de l'article 2 alinéa 2 de l'arrêté du 15 janvier 2002 relatif à l'ARTT, 5 jours au titre de l'alinéa 3 du même article), desquels est déduite une journée de solidarité. Cette journée est déclarée par l'agent au moment de l'établissement du planning, soit au moyen du don d'un jour de congé, soit en signalant sa participation à une action en dehors de son planning.

Les personnels contractuels dont le temps de travail hebdomadaire est fixé à 35h bénéficient de 2,5 jours de congé par mois de travail.
Le droit à congé des agents exerçant à temps partiel est calculé en proportion de leurs obligations de service.
La gestion des congés est informatisée.
Dans l'outil, les jours ARTT ne sont pas différenciés des jours de congés annuels.

La période de référence est l'année universitaire, du 1er septembre au 31 aout de l'année N+1.

Le décompte des congés s'effectue par demi-journée pour l'ensemble des agents. Les agents sont invités à déposer un calendrier prévisionnel de congé au fur et à mesure qu'il les soumettra à validation.

4.2. Conditions d'octroi et d'utilisation

4.2.1 Conditions d'octroi

L'octroi des congés fait nécessairement l'objet d'une demande préalable auprès du responsable de service.
Un délai de prévenance de 10 jours doit être respecté. Les congés sont accordés sous réserve des nécessités du service.

4.2.2 Conditions d'utilisation

Pour le Personnel 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.

Pour le personnel Université : Les agents doivent avoir apuré leurs congés avant le 31 août de l'année N+1. Un reliquat de 5 jours peut être reporté et pris entre le 1er septembre et le 31 décembre de l'année N+1. Au-delà de cette date, les congés non consommés sont perdus.

4.3 Journée de solidarité

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

Pour le personnel CNRS et IRD : Cette journée prend obligatoirement la forme d'un jour RTT déduit en début d'année de votre contingent annuel de jours RTT.
Pour un agent à temps partiel, le nombre d'heures dû au titre de la journée de solidarité est proratisé en fonction de sa quotité de temps de travail et donne lieu à une récupération en temps de repos du temps supplémentaire accompli par rapport à la valeur horaire d'un jour RTT
Exemples : un agent à 80% travaillant sur 4 jours doit accomplir une journée de solidarité de 5 heures 36 minutes (7*0,8). La valeur horaire de sa journée RTT est de 7h42. L'agent a droit à une récupération de 2 heures 6 minutes (7h42 – 5h36).
La journée de solidarité doit être déduite pour les agents présents du 01/01 au 31/12 de l'année en cours.

Pour le personnel Université : Cette journée est déclarée par l'agent au moment de l'établissement du planning, soit au moyen du don d'un jour de congé, soit en signalant sa participation à une action en dehors de son planning.
La réalisation de la journée de solidarité (7 heures) doit obligatoirement se faire par fraction minimum de travail d'une demi-journée (2 X 3 heures 30 ou 3 heures + 4 heures) à prendre sur les congés supplémentaires au titre de l'ARTT ou sur les heures supplémentaires réalisées dans l'année universitaire. La déclaration de votre journée de solidarité se fera dans l'application E-grh afin de donner un jour de congé au titre de la journée de solidarité ou de renseigner votre « action » (un jour ou deux demi -journées) en dehors de votre planning (INFOSUP, Journée porte ouverte...). Si votre quotité de travail est inférieure à 100%, vous déclarerez une demi-journée.
Cette évolution vise notamment à harmoniser les pratiques entre services et a fait l'objet d'un avis favorable du Comité Technique Paritaire du 28 septembre 2009. Elle n'a pas pour effet d'augmenter le temps de travail global.
S'agissant des agents exerçant leurs fonctions à temps partiel et à temps incomplet, les sept heures de cette journée de travail sont proratisées par rapport à la quotité de ce temps de travail correspondante.

4.4. Compte épargne temps (CET)

Tout agent titulaire ou non titulaire de l'Unité, employé de manière continue depuis au moins un an dans une administration de l'Etat, un établissement public à caractère administratif de l'Etat ou un établissement public local d'enseignement, peut ouvrir un CET.
Les conditions d'alimentation et d'utilisation du CET sont fixées par le décret n°2002-634 du 29 avril 2002 modifié et par son arrêté d'application du 20 janvier 2004 modifié.

Pour le personnel CNRS et IRD :
Le CET peut être alimenté sur le logiciel AGATE (gestion des congés). La gestion et le suivi du CET sont confiés au service des ressources humaines de la délégation régionale du CNRS.
Pour le personnel de l'Université (hors enseignants-chercheurs) :
Le CET est un dispositif permettant aux agents de ne pas perdre les congés qui n'ont pu être pris.
La situation selon laquelle l'aménagement du temps de travail mis en place dans une structure génère pour un agent un régime de jours de congés plus favorable que les 45 jours prévus réglementairement et qu'il n'en aurait pas bénéficié en totalité est sans incidence sur le mode de calcul du nombre de jours qu'il est en droit d'épargner.
Le dispositif s'applique aux personnels BIATSS :

- Titulaires
- Non-titulaires recrutés sur contrat de droit public ayant accompli au moins une année de service public de manière continue au moment de la demande d'ouverture du compte.

Les personnels stagiaires ne sont pas concernés.
La campagne d'alimentation a lieu chaque année entre le 1er novembre et le 31 décembre.
Il convient à cet égard de veiller à ce que les agents puissent prendre la majorité de leurs congés annuels de manière régulière pour éviter des difficultés de fonctionnement ultérieures.
Tout au long de l'année, l'agent peut demander à utiliser les jours stockés sur le CET sous forme de congés.

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.

5.2. Autorisation exceptionnelle d'absence :

Les autorisations exceptionnelles d'absences sont :
- des autorisations spéciales d'absence, de droit, autorisées en application des textes. (**cf. Annexe 5 – autorisations exceptionnelles d'absences**)
- des autorisations d'absences dites mesures de « bienveillance », accordée sous réserve des nécessités de service par le directeur de l'Unité.

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.
La règlementation impose l'autorisation préalable du fonctionnaire sécurité défense pour les missions des agents dans certains pays étrangers (voir liste établie par le ministère des affaires étrangères).
L'agent amené à se rendre directement de son domicile sur un lieu de travail occasionnel sans passer par sa résidence administrative habituelle doit nécessairement être en possession d'un ordre de mission.

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

Chapitre 3 : Santé et sécurité

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

7.1 Directeur d'Unité

Le Directeur d'Unité doit veiller à la sécurité et à la protection des agents placés sous son autorité et d'assurer la sauvegarde des biens dont il dispose. (**Annexe 6 - Consignes de sécurité)**

7.2 Assistant de prévention (AP)

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.
(**Annexe 7 - Rôle et mission de l'assistant de prévention**)

7.3 Equipiers de sécurité Incendie

Les noms, coordonnées et localisations des équipiers de 1ère intervention et chargés d'évacuation (guide-file, serre-file) figurent en **annexe 8 - Personnes ressources en matière de sécurité et de prévention des risques**.

7.4 Personnes compétentes dans un domaine de gestion du risque

Les noms et les coordonnées de ces personnes sont données dans **l'annexe 8 - Personnes ressources en matière de sécurité et de prévention des risques.**

- Personne compétente en radioprotection (PCR)
- Deux assistants de prévention (risques chimiques ; risques mécaniques et appareillages sous pression)
- Référent sécurité LASER
- Responsable de gestion de déchets

7.5 Membres de l'instance de concertation

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 :

- Arrêté N° 2012-001 Création d'un CHSCT d'établissement au sein de l'Université Blaise Pascal Clermont-Ferrand II
- Décision de création des CRHSCT régionaux (DEC121279DRH)

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 situé à l'infirmerie du Campus des Cézeaux.
Médecin de prévention (personnel CNRS) : **Dr Laurette ROCHER** 04 72 69 26 76
Médecin de prévention (personnel Université) : **Dr M. C. RATINAUD**

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

• Laboratoires de chimie incluant la salle blanche et les salles de chimie grises. Les risques spécifiques sont ceux associés à la manipulation d'acides et de bases concentrés (brûlures cutanées, projections oculaires, inhalation de vapeurs acides). En prévention, l'air des salles est renouvelé en continu, des hottes aspirantes et des équipements de protection individuels (EPI) sont à disposition (blouses, gants, lunettes, masques de protection du visage, masques filtrant les vapeurs acides).

• Laboratoires de pétrologie expérimentale. Les risques découlent de l'utilisation d'instruments mettant en jeu des solides ou des gaz sous pression (presses, piston-cylindres, autoclaves), de fours et de rayons laser : blessures physiques, brûlures et atteintes oculaires (laser). Des EPI (lunettes, gants) sont à disposition.

• Laboratoires de volcanologie expérimentale. Les risques découlent du travail en hauteur (échelle), de l'utilisation de poudres de faible granulométrie pour étudier les écoulements granulaires et de la manipulation de masses significatives (kg) de produits chauffés.

• Laboratoires de séparation minérale. Les risques concernent la manipulation de solvants organométalliques toxiques. Les manipulations de solvant sont réalisées sous hotte aspirante et des EPI (gants, masques) sont utilisés.

• Ateliers de sciage-broyage. Les risques concernent l'utilisation des scies et des instruments de broyage (blessure physique) et du bruit généré (acouphènes). Les machines sont équipées de systèmes de sécurité et des EPI sont à disposition.

• Atelier de mécanique. Les risques découlent de l'utilisation des instruments d'usinage (blessure physique) et du bruit généré (acouphènes). Les machines-outils sont équipées de systèmes de sécurité. Des EPI sont mis à disposition (chaussures de sécurité, bleu de travail, casque anti-bruit, gants). Une trousse de premier soin est présente.

• Missions sur le terrain
Lors de la réalisation de mission de terrain en milieu isolé, toutes les personnes participant à la mission doivent, autant que possible, avoir suivi une formation au secourisme en milieu isolé. Ils partent avec une trousse à pharmacie dite « milieu isolé ». En outre, ils ont la possibilité d'emporter un téléphone satellite pour prévenir les secours. Les missions en terrain difficile ne pourront être réalisées qu'en équipe de plusieurs personnes.
Pour les missions en altitude > 3500 m, les agents doivent effectuer une visite médicale et un test d'aptitude au travail en altitude. Ils sont invités à prendre connaissance des risques et des moyens de

prévention dans le livret mis à leur disposition à l'entrée du laboratoire (http://www.dgdr.cnrs.fr/sst/cnmp/documents/Livret%20haute%20altitude_2016%2007%2005%20V8b%20Final.pdf)

L'ensemble des laboratoires se trouve dans une partie du bâtiment accessible par badge uniquement. L'accès aux laboratoires est contrôlé par digicode ou fermeture à clef. L'accès est autorisé uniquement aux personnes compétentes. Dans le cadre de la formation à la sécurité (cf. point 8.6) les nouveaux-entrants reçoivent une formation spécifique adaptée à leur poste de travail.

8.3 Organisation des secours

La procédure d'organisation des secours est fixée par l'Université Clermont Auvergne. Dès l'audition du signal sonore ou sur ordre, le personnel doit évacuer les bâtiments et se regrouper sur les lieux prévus à cet effet, matérialisés par un pictogramme. Le rythme des exercices d'évacuation et d'environ un tous les deux ans. Tout le personnel doit participer à cet exercice d'évacuation.

Les numéros d'appel d'urgence sont :
Poste de secours : 42
Pompiers : 18
SAMU : 154
Police : 17

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

La procédure d'organisation des secours est fixée par l'Université Clermont Auvergne. Dès l'audition du signal sonore ou sur ordre, le personnel doit évacuer les bâtiments et se regrouper sur les lieux prévus à cet effet, matérialisés par un pictogramme (Deux points de rassemblement : à l'entrée principale, et sur parking à l'entrée sud). Le rythme des exercices d'évacuation et d'environ un tous les deux ans. Tout le personnel doit participer à cet exercice d'évacuation.

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 par l'assistant de prévention. Selon les cas, il pourra s'entourer de toute personne compétente, après avis du Directeur de l'Unité.

8.6 Formation à la sécurité

Tout nouvel entrant reçoit une formation relative à la sécurité et, le cas échéant, une formation spécifique adaptée à son poste de travail. Les formations sont dispensées en concertation avec les assistants de prévention, et leur fréquence est adaptée au calendrier/rythme des arrivées.

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. Le registre santé sécurité au travail se situe **dans le couloir « Administration-Direction » au rez-de-chaussée du bâtiment**.

8.8 Accueil de personnes extérieures

- Stagiaires et visiteurs

Un accueil personnalisé est réalisé lors de l'arrivée du stagiaire ou visiteur. Un parcours d'accueil est proposé.

- 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 est réalisé. Les personnes concernées par ce plan de prévention sont : l'entreprise extérieure, la personne demandant les travaux dans l'Unité et les assistants de prévention.

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 (**cf. Annexe 9 - Note sur le travail isolé**).
En dehors des heures ouvrables, l'utilisation des laboratoires présentant des risques (chimie, pétrologie expérimentale, et volcanologie expérimentale) est autorisée ponctuellement, uniquement :
- en présence d'une seconde personne compétente, ou,
- en prévenant une seconde personne compétente qui s'assurera à distance du bon déroulé de l'intervention

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.

9.4 Stupéfiants

Il est interdit de pénétrer ou de demeurer dans l'Unité sous l'emprise de stupéfiants.
Le Directeur d'Unité doit retirer de son poste de travail toute personne étant sous l'emprise apparente de stupéfiants sur un poste dangereux pour sa santé et sa sécurité, ainsi que pour celles des autres personnes placées à proximité.

9.5 Véhicules de service.
Seuls peuvent utiliser les véhicules de service les personnels de l'unité ayant un permis de conduire valide et ayant reçu l'autorisation du responsable des tutelles, sur proposition du directeur d'unité.
Pour les véhicules CNRS, les personnes ont interdiction de transporter du personnel étranger au service. Par conséquent, tout covoiturage est interdit avec les véhicules de service et de location. Pas d'interdiction particulière pour les véhicules de l'UCA. Ceux-ci doivent être employés dans les conditions normales du service.

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.

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, le cas échéant après autorisation du Directeur de l'Unité et du responsable scientifique du projet, 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 (Protection du Potentiel Scientifique et Technique) applicable lorsque le sujet de la publication relève d'un secteur protégé,
- les droits d'auteurs sur les textes, images, sons, vidéos...

10.2.2 Formalisme des publications et communication

Les publications des personnels de l'Unité font apparaître le lien avec les organismes de tutelle. L'affiliation correspond aux dispositions de la convention quinquennale en vigueur. La signature doit se présenter sous cette forme :

Nom, Prénom, Université Clermont Auvergne, CNRS, IRD, OPGC, Laboratoire Magmas et Volcans, F-63000 Clermont-Ferrand, France

Un exemplaire de toutes les publications (articles, revues, thèses…) dont tout ou partie du travail a été effectué à l'Unité doit être remis dès parution au service de documentation.

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.

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 Site web du LMV

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.

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 et la charte graphique des autres tutelles le cas échéant.

Le site internet du LMV est sous la responsabilité du Directeur de l'Unité. Par délégation, la cellule de communication est en charge d'actualiser et modifier son contenu.

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.

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 ces collaborations nécessitent avant signature l'autorisation formelle du ministère de tutelle, et de toute demande de subvention de l'Unité par 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 les personnels IRD, les sanctions sont notifiées par le directeur du département.

Pour l'établissement l'UCA, 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.

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 (**Annexe 10 - Charte Informatique de l'OPGC**).

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.

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.

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. (**cf. Annexe 11 - PSSI Opérationnelle de l'unité**)

Article 14 : Utilisation des ressources techniques collectives

L'accès à la bibliothèque et à la lithothèque est strictement réservé aux membres du laboratoire, ou aux visiteurs scientifiques. Tout nouvel arrivant doit s'adresser à la personne en charge de la bibliothèque, qui lui expliquera le fonctionnement des services.

L'utilisation des équipements dans les services communs est régie par les responsables des services. L'utilisation des instruments dans les laboratoires est organisée par les responsables des instruments et supervisée par les responsables d'équipe (http://lmv.univ-bpclermont.fr/recherche/instruments/).

Article 15 : Durée

Le règlement intérieur entre en vigueur à la date de signature par le Délégué régional du CNRS et par les 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 et sur l'intranet du laboratoire.
Il annule et remplace le règlement intérieur de 18/01/2011 et entre en vigueur au **1er septembre 2017**.

Fait à Aubière, le 19 juin 2017

Signature des représentants légaux des tutelles

Visa du Directeur de l'Unité

UMR6524
Visa du *Directeur de l'Unité*, **M. Didier LAPORTE**
Date :
Signatures & tampon

CNRS Délégation DR07 Rhône Alpes
Visa de **M. Frédéric FAURE**, *Délégué Régional Rhône Auvergne*
Date :
Signatures & tampon.

UNIV CLERMONT AUVERGNE
Visa de **M. Mathias BERNARD**, *Président*
Date :
Signatures & tampon.

IRD
Visa de **M. Jean-Paul MOATTI**, *Président-Directeur Général*
Date :
Signatures & tampon.

Règlement intérieur de l'Université Jean Monet

En attente de validation

COMPOSITION DU CONSEIL DE LABORATOIRE

Membres de droit

Directeur, **Didier Laporte**
Directeur-adjoint, **Ivan Vlastelic**
Directeur-adjoint IRD, **Olivier Roche**
Directeur-adjoint technique, **Jean-Louis Paquette**

Membres nommés par le Directeur du Laboratoire

Responsable de l'équipe de pétrologie, **Nathalie Bolfan**
Responsable de l'équipe de géochimie, **Maud Boyet**
Responsable de l'équipe de volcanologie, **Raphael Paris**
Représentant de l'antenne stéphanoise, **Damien Guillaume**

Membres élus

Collège des chercheurs

Rang A :

Timothy Druitt
Lucia Gurioli

Rang B :

Tahar Hammouda
Julien Monteux

Sous collège Post-Doctorants
Mickael Laumonier

Sous collège *Doctorants*
Pierre Faure

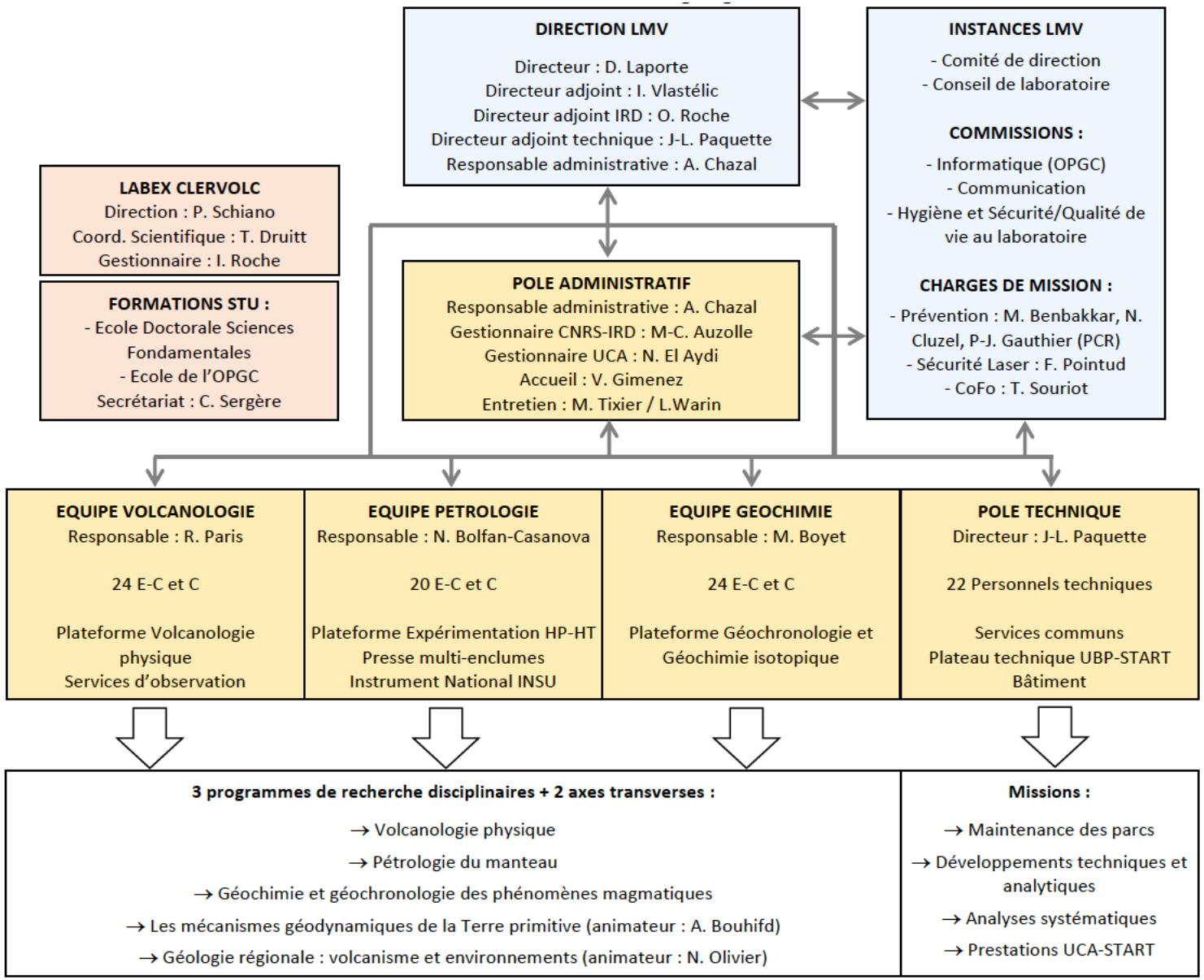
Collège des ITA – IATOS

Claire Fonquernie
Mouhcine Gannoun
Krzysztof Suchorski

Invités permanents

Directeur de l'OPGC, **Patrick Bachèlery**
Directeur du Labex Clervolc, **Pierre Schiano**
Responsable de l'axe transverse « Géologie régionale »**, Nicolas Olivier**
Responsable de l'axe transverse « Terre primitive », **Ali Bouhifd**
Responsable administrative, **Audrey Chazal**
Directeur-adjoint de l'OPGC en charge des formations, **Thierry Menand**
Représentant « Magmas et Volcans » de l'Ecole doctorale Sciences Fondamentales, **Hervé Martin**

ANNEXE N°3 : Organigramme LMV 2017-2021



ANNEXE N°4 : Deliberation-ca-2017-05-19-01-temps-de-travail pour les personnels BIATSS UCA

UNIVERSITÉ Clermont Auvergne

CONSEIL D'ADMINISTRATION
DELIBERATION N° 2017-05-19-01

DELIBERATION DU CONSEIL D'ADMINISTRATION DE L'UNIVERSITE CLERMONT AUVERGNE PORTANT ORGANISATION DU TEMPS DE TRAVAIL DES PERSONNELS BIATSS

LE CONSEIL D'ADMINISTRATION DE L'UNIVERSITE CLERMONT AUVERGNE, EN SA SEANCE DU 19 MAI 2017,

Vu le code de l'Education,
Vu le décret n°84-972 du 26 octobre 1984 relatif aux congés annuels des fonctionnaires de l'Etat,
Vu le décret n°2000-815 du 25 août 2000 relatif à l'aménagement et à la réduction du temps de travail dans la fonction publique de l'Etat et dans la magistrature,
Vu le décret 2015-580 permettant à un agent public civil le don de jours de repos à un autre agent public parent d'un enfant gravement malade,
Vu l'arrêté du 15 janvier 2002 portant application du décret n°2000-815 du 25 août 2000 relatif à l'aménagement et à la réduction du temps de travail dans les services déconcentrés et établissements relevant du ministère de l'éducation nationale,
Vu l'arrêté du 15 janvier 2002 portant application du décret n°2000-815 du 25 août 2000 et relatif à l'organisation du travail dans les services déconcentrés et établissements relevant du ministère de l'éducation nationale,
Vu la circulaire FP n°1475 du 20 juillet 1982,
Vu la circulaire n°2002-007 du 21 janvier 2002, parue au BOEN spécial du 7 février 2002,
Vu la circulaire n° 2010-205 du 17 septembre 2010, parue au BOEN du 4 novembre 2010,
Vu la circulaire DGAFP NOR MFPF1202031C du 18 janvier 2012 relative aux modalités de mise en œuvre de l'article 115 de la loi n° 2010-1657 du 29 décembre 2010 de finances pour 2011,
Vu les statuts de l'Université Clermont Auvergne, adoptés par délibération du 7 octobre 2016,
Vu la délibération 2016-11-29-04 de l'assemblée constitutive provisoire,
Vu l'avis du comité technique du 16 mai 2017,

Vu la présentation de Monsieur le Président de l'université Clermont Auvergne,

APRES avoir délibéré,

DECIDE

D'adopter l'organisation du temps de travail des personnels BIATSS de l'université Clermont Auvergne comme suit :

Article 1 : Durée
La base annuelle de travail est de 1 593 heures pour l'ensemble des personnels (1607 heures – 14 heures de fractionnement des congés) à l'exception des personnels d'accueil logés par nécessité absolue de service en poste simple, pour qui le temps de travail est fixé à 1 716 heures.

L'horaire hebdomadaire est fixé à :

- 37 heures 30 pour l'ensemble des agents titulaires et agents non titulaires recrutés sur contrat à durée déterminée supérieure à 10 mois à l'exception des personnels logés chargés de l'accueil, des personnels de santé et des contractuels recrutés sur contrat à durée inférieure ou égale à 10 mois ;
- 38 heures 10 pour les personnels de la BCU ;

- 35 heures pour les personnels techniques et administratifs recrutés sur contrat à durée inférieure ou égale à 10 mois.

Article 2 : Eléments constitutifs de l'emploi du temps
L'emploi du temps est mis en œuvre pour la période allant du 1er septembre au 31 août de l'année suivante.
L'emploi du temps est proposé par l'agent puis validé par le chef de service, l'organisation du travail retenue devant permettre d'offrir aux usagers un service optimal.
La semaine d'activité se répartit sur cinq journées au moins pour les agents exerçant à 90% ou 100%.
La durée journalière de travail est au minimum de 5 heures.
La demi-journée est une plage horaire d'une durée inférieure à 5 heures. Le travail en demi-journée ne peut concerner que les agents à temps partiel ou incomplet.
La journée de travail est répartie sur deux plages horaires, à l'exception de la journée contractée.
L'amplitude journalière maximale est de onze heures, coupure éventuelle comprise.

Pour les personnels dont le temps de travail quotidien atteint six heures, la durée journalière comprend une pause de 20 minutes considérée comme temps travaillé.

L'établissement propose à tous les agents la possibilité d'avoir des emplois du temps différents selon les périodes de l'année, dans le respect de la durée annuelle du temps de travail.
La fourchette, variable selon les filières, s'établit ainsi :
- Filières administrative, bibliothèque, recherche et formation : 32 heures – 40 heures ;
- Filières sociale et santé : 32 heures – 44 heures.

Les pics d'activité correspondent aux semaines de travail atteignant le maximum de l'amplitude hebdomadaire, dans la limite de 8 semaines par an et sous réserve qu'elles correspondent à une véritable charge de travail clairement identifiée.
Ces modulations, qui doivent être prévues dès le début d'année universitaire, ne peuvent en aucun cas être imposées à l'agent.

Article 3 : journée contractée :
Les agents à temps complet, avec l'accord de leur supérieur hiérarchique, peuvent bénéficier d'une journée hebdomadaire contractée de 5 heures, conformément aux dispositions adoptées par l'assemblée constitutive provisoire le 29/11/2016.

Article 4 : Pause méridienne :
La pause méridienne est comprise entre 45 minutes et 2 heures.

Article 5 : Congés et ARTT
Le nombre total de jours alloués à l'agent à temps complet est de 50 (25 jours de congés annuels au titre du décret 84-972, 20 jours au titre de l'article 2 alinéa 2 de l'arrêté du 15 janvier 2002 relatif à l'ARTT, 5 jours au titre de l'alinéa 3 du même article), desquels est déduite une journée de solidarité. Cette journée est déclarée par l'agent au moment de l'établissement du planning, soit au moyen du don d'un jour de congé, soit en signalant sa participation à une action en-dehors de son planning (type portes ouvertes).
Les personnels de la Bibliothèque Clermont Université, dont le temps de travail hebdomadaire est de 38h10, bénéficient de 54 jours, journée de solidarité déduite.
Les personnels contractuels dont le temps de travail hebdomadaire est fixé à 35h bénéficient de 2,5 jours de congé par mois.
Le droit à congé des agents exerçant à temps partiel est calculé en proportion de leurs obligations de service.
La gestion des congés est informatisée.
Dans l'outil, les jours d'ARTT ne sont pas différenciés des jours de congés annuels.
La période de référence est l'année universitaire, du 1er septembre au 31 août de l'année N + 1.
Les agents doivent avoir apuré leurs congés avant le 31 août de l'année N+1. Un reliquat de 5 jours peut être reporté et pris entre le 1er septembre et le 31 décembre de l'année N+1. Au-delà de cette date, les congés non consommés sont perdus.

Le décompte des congés s'effectue par demi-journée pour l'ensemble des agents. Par exception, les personnels de la Bibliothèque Clermont Université se voient appliquer un décompte horaire.
Le décompte horaire a vocation à être généralisé à l'ensemble de l'établissement, dès que le développement de l'outil informatique le permettra.

Les agents sont invités à déposer un calendrier prévisionnel de congés. L'agent pourra, en lien avec son supérieur hiérarchique, ajuster les périodes de congé au fur et à mesure qu'il les soumettra à validation.

Article 6 : Compte épargne temps :

Le CET est un dispositif permettant aux agents de ne pas perdre les congés qui n'ont pas pu être pris.
La situation selon laquelle l'aménagement du temps de travail mis en place dans une structure génère pour un agent un régime de jours de congés plus favorable que les 45 jours prévus réglementairement et qu'il n'en aurait pas bénéficié en totalité est sans incidence sur le mode de calcul du nombre de jours qu'il est en droit d'épargner.
Le dispositif s'applique aux personnels BIATSS :

- titulaires
- non-titulaires recrutés sur contrat de droit public ayant accompli au moins une année de service public de manière continue au moment de la demande d'ouverture du compte.

Les personnels stagiaires ne sont pas concernés.
La campagne d'alimentation a lieu chaque année entre le 1er novembre et le 31 décembre.
Il convient à cet égard de veiller à ce que les agents puissent prendre la majorité de leurs congés annuels de manière régulière pour éviter des difficultés de fonctionnement ultérieures.
Tout au long de l'année, l'agent peut demander à utiliser les jours stockés sur le CET sous forme de congés.

Article 7 : heures supplémentaires

Les heures supplémentaires effectives sont les heures supplémentaires en dépassement du plafond hebdomadaire défini pour la semaine considérée, et à la demande du supérieur hiérarchique direct qui valide le besoin, autant que possible en amont.

Le total ne saurait excéder 140h par an.
Le suivi des heures supplémentaire est effectué par le supérieur hiérarchique.
La récupération des heures supplémentaires doit intervenir dans le semestre qui suit, et être validée par le chef de service.
L'attention des chefs de service est appelée sur les conséquences sur l'organisation ultérieure que peuvent avoir les cumuls importants d'heures supplémentaires.

Article 8 : Calcul du droit à congés en cas d'absence prolongée pour raison de santé

A partir de 10 jours ouvrés d'absence sur la période de référence, entendue du 1er septembre de l'année N au 31 août de l'année N+1, le droit à congés des agents est modifié comme suit :
10 à 19 jours d'absence : 49 moins la journée de solidarité
20 à 29 jours d'absence : 48 moins la journée de solidarité
30 à 39 jours d'absence : 47 moins la journée de solidarité
40 à 49 jours d'absence : 46 moins la journée de solidarité
50 à 59 jours d'absence : 45 moins la journée de solidarité
60 à 69 jours d'absence : 44 moins la journée de solidarité
70 à 79 jours d'absence : 43 moins la journée de solidarité
80 à 89 jours d'absence : 42 moins la journée de solidarité
90 à 99 jours d'absence : 41 moins la journée de solidarité
100 à 109 jours d'absence : 40 moins la journée de solidarité
110 à 119 jours d'absence : 39 moins la journée de solidarité
120 à 129 jours d'absence : 38 moins la journée de solidarité
130 à 139 jours d'absence : 37 moins la journée de solidarité
140 à 149 jours d'absence : 36 moins la journée de solidarité
150 à 159 jours d'absence : 35 moins la journée de solidarité
160 à 169 jours d'absence : 34 moins la journée de solidarité
170 à 179 jours d'absence : 33 moins la journée de solidarité
180 à 189 jours d'absence : 32 moins la journée de solidarité
190 à 199 jours d'absence : 31 moins la journée de solidarité
200 à 209 jours d'absence : 30 moins la journée de solidarité
210 à 219 jours d'absence : 29 moins la journée de solidarité
220 à 229 jours d'absence : 28 moins la journée de solidarité
230 à 239 jours d'absence : 27 moins la journée de solidarité
A partir de 240 : 26 moins la journée de solidarité

Article 9 : autorisations d'absence pour soigner un enfant malade ou en assurer momentanément la garde
Les agents ayant un ou plusieurs enfant(s) à charge peuvent bénéficier, sous réserve des nécessités de service, d'autorisations d'absence pour leur donner des soins ou en assurer la garde de façon ponctuelle.
Dans tous les cas, un justificatif (certificat médical...) permettant d'établir l'exactitude matérielle du motif invoqué doit être fourni à l'appui de la demande transmise, par la voie hiérarchique, à la Direction des Ressources Humaines.
Les rendez-vous médicaux n'entrent pas dans ce cadre, sauf présentation d'un justificatif.
L'âge limite des enfants pour lesquels ces autorisations d'absence peuvent être accordées est de seize ans, aucune limite d'âge n'étant fixée pour les enfants handicapés.
La durée totale des autorisations ne pourra pas dépasser, chaque année :

- 6 jours pour un agent à temps complet,
- 12 jours pour un agent à temps complet assumant seul la charge de son (ses) enfant(s) **ou** dont le conjoint est à la recherche d'un emploi **ou** dont le conjoint ne bénéficie d'aucune autorisation analogue : dans ces deux derniers cas, il convient de fournir un justificatif.

Pour les agents exerçant à temps partiel, le plafond des autorisations d'absence est fonction de la quotité.

Article 10 : don de jours de congés pour un collègue dont l'enfant est gravement malade
Aux termes du décret 2015-580, un agent public civil peut, sur sa demande, renoncer anonymement et sans contrepartie à tout ou partie de ses jours de repos non pris, qu'ils aient été affectés ou non sur un compte épargne-temps, au bénéfice d'un autre agent public relevant du même employeur, qui assume la charge d'un enfant âgé de moins de vingt ans atteint d'une maladie, d'un handicap ou victime d'un accident d'une particulière gravité rendant indispensables une présence soutenue et des soins contraignants.

Les jours qui peuvent faire l'objet du don sont les suivants :
Jours de congés : tout ou partie des jours excédant 20 jours ouvrés
Jours d'ARTT : tout ou partie
Les jours de repos compensateur et les congés bonifiés n'entrent pas dans ce champ.

Peuvent être bénéficiaires les agents publics (titulaires et contractuels) ayant épuisé leurs congés et parents d'un enfant gravement malade, handicapé ou accidenté.
Les bénéficiaires doivent relever du même employeur que les donateurs.

La rémunération de l'agent bénéficiaire est maintenue pendant le congé, qui est considéré comme une période de service effectif.
La durée est plafonnée à 90 jours par enfant et par année civile.
Par dérogation, l'absence du service des agents publics civils bénéficiaires d'un don de jours de repos au titre du présent décret peut excéder trente et un jours consécutifs.

L'agent donateur fait part de son souhait par écrit et par voie hiérarchique auprès de la Direction des Ressources Humaines.
Cette demande doit comporter le nombre de jours qu'il envisage de donner, ainsi que la nature de ces jours.
Le don de jours épargnés sur un CET est possible à tout moment.
Le don de jours non épargnés sur un CET peut être fait jusqu'au 31 décembre de l'année au titre de laquelle les jours de repos sont acquis.

La Direction des Ressources Humaines vérifie que les conditions sont remplies pour le don et notifie sa décision au donateur.
Le cas échéant, les jours donnés sont alors retirés du CET et/ou du compte de congés de l'agent.
La Direction des Ressources Humaines assure le suivi des jours versés et en rend compte au moins annuellement au Comité Technique. Cette donnée figure dans le bilan social.

L'agent qui souhaite bénéficier d'un don en fait la demande par écrit, en joignant un certificat médical détaillé remis sous pli confidentiel établi par le médecin qui suit l'enfant et attestant la particulière gravité de la maladie, du handicap ou de l'accident rendant indispensables une présence soutenue et des soins contraignants auprès de l'enfant.
La Direction des Ressources Humaines vérifie l'éligibilité réglementaire de la demande.
Elle réunit ensuite une commission composée :

- du médecin de prévention, seul-e habilité-e à prendre connaissance des éléments portés sur le certificat médical,

- de l'assistant-e de service social des personnels,
- du/de la directeur-trice des ressources humaines ou son-sa représentant-e,
- d'un-e représentant-e élu-e des personnels

Au vu de l'avis de la commission, la Direction des Ressources Humaines notifie la décision du Président à l'agent demandeur.
Elle crédite le compte « egrh » de l'agent du nombre de jours accordés.

Si l'intégralité des jours attribués n'a pas été consommée, la Direction des Ressources Humaines retire ces jours du compte « egrh » de l'agent et les rétablit dans le stock de jours pouvant faire l'objet d'un don.

Article 11 : périodes de fermeture de l'établissement

Le conseil d'administration décide annuellement, sur avis du comité technique, des périodes de fermeture hivernale et estivale de l'établissement.
Pendant ces périodes, les personnels ne travaillent pas.
Les chefs de service ont la possibilité de demander une dérogation en cas de nécessité de service.

Membres en exercice : 37
Votes : 31
Pour : 28
Contre : 0
Abstentions: 3

Le Président,

Mathias BERNARD

CLASSE AU REGISTRE DES ACTES SOUS LA REFERENCE : CA UCA 2017-05-19-01

TRANSMIS AU RECTEUR : 22/05/2017

PUBLIE LE : 22/05/2017

Modalités de recours : *En application de l'article R421-1 du code de justice administrative, le Tribunal Administratif de Clermont-Ferrand peut être saisi par voie de recours formé contre les actes réglementaires dans les deux mois à partir du jour de leur publication et de leur transmission au Recteur.*

ANNEXE N°5 : AUTORISATIONS D'ABSENCE

MOTIF	DUREE	TEXTES DE REFERENCE	JUSTIFICATIFS	COMMENTAIRES
POUR RAISONS FAMILIALES OU RELIGIEUSES				
Mariage / P.A.C.S de l'agent	5 jours ouvrables	Instruction n°7 du 23 mars 1950 Circulaire FP/7 n°002874 du 7 mai 2001	Copie de l'extrait d'acte de mariage / P.A.C.S	Mesure de bienveillancerelevant de l'appréciation du chef de service. En cas de déplacement à effectuer, la durée d'absence peut être majorée des délais de route sans pouvoir excéder 48h aller-retour
Naissance / adoption	3 jours ouvrables pour le père, consécutifs ou non et devant être pris dans les 15 jours suivants la naissance / l'arrivée de l'enfant	Loi du 18 mai 1946 Instruction n°7 du 23 mars 1950	Copie de l'extrait d'acte de naissance	Congé supplémentaire. Aucune majoration en cas de naissance ou d'adoption multiple
Paternité	11 jours (qui s'ajoutent au congé de naissance supra), consécutifs et non fractionnables, devant être pris dans les 4 mois suivant la naissance de l'enfant. En cas de naissance multiple, le congé est étendu à 18 jours. Les mêmes règles s'appliquent au congé d'adoption.	Loi 2001-1246 du 21 décembre 2001 Décrets du 28 décembre 2001 Circulaire FP/3 - FP/4 n°2018 du 24 janvier 2002	Copie de l'extrait d'acte de naissance. La demande doit être effectuée par l'agent au moins 1 mois avant la date à laquelle il entend prendre son congé	Mesure de bienveillance relevant de l'appréciation du chef de service. Ces jours doivent être consécutifs donc non fractionnables
Rentrée scolaire (pré-élémentaire, élémentaire et entrée en 6ème) d'un enfant dont l'agent assume la garde	Facilités d'horaires	Circulaire à consulter chaque année durant les congés scolaires d'été		Mesure de bienveillance relevant de l'appréciation du chef de service. Absences accordées dans la mesure où elles sont compatibles avec le fonctionnement normal du service
Participation à des fêtes ou cérémonies religieuses non inscrites au calendrier des jours chômés	Liste à consulter chaque année, en novembre, au Bulletin Officiel de l'Education Nationale	Circulaire FP n°901 du 23 septembre 1967	Tout justificatif	Mesure de bienveillance relevant de l'appréciation du chef de service. Absences accordées dans la mesure où elles sont compatibles avec le fonctionnement normal du service
POUR RAISONS DE SANTE				
Décès ou maladie très grave du conjoint, père, mère et enfant	3 jours ouvrables	Instruction n°7 du 23 mars 1950 Circulaire FP/7 n°002874 du 7 mai 2001	Copie de l'acte de décès/certificat médical	Mesure de bienveillance relevant de l'appréciation du chef de service. En cas de déplacement à effectuer, la durée d'absence peut être majorée des délais de route sans pouvoir excéder 48h aller-retour
Soins ou garde momentanée d'enfant de moins de 16 ans	1 fois les obligations hebdomadaires de service + 1 jour, soit : - 6 jours ou 12 demi-journées pour un 100% - 5,5 jours ou 11 demi-journées pour un 90% - 5 jours ou 10 demi-journées pour un 80% - 4,5 jours ou 9 demi-journées pour un 70% - 4 jours ou 8 demi-journées pour un 60% - 3,5 jours ou 7 demi-journées pour un 50%	Circulaire FP n°1475 et B-2A/98 du 20 juillet 1982 Circulaire n°83-164 du 13 avril 1983	Certificat médical ou justificatif	Le nombre de jours est doublé dans les cas suivants : - l'agent élève seul(e) son enfant - son conjoint est en recherche d'emploi (attestation ANPE) - son conjoint ne bénéficie pas d'autorisation d'absence rémunérée (attestation de l'employeur)

ANNEXE N°5 : AUTORISATIONS D'ABSENCE

MOTIF	DUREE	TEXTES DE REFERENCE	JUSTIFICATIFS	COMMENTAIRES
Séances préparatoires à l'accouchement sans douleurs	Durée des séances	Circulaire FP/4 n°1864 du 9 août 1995	Sur avis du médecin chargé de la prévention au vu des pièces justificatives	Mesure de bienveillance relevant de l'appréciation du chef de service. L'autorisation d'absence peut être accordée lorsque les séances ne peuvent avoir lieu en dehors des heures de travail
Allaitement	Dans la limite d'1 heure par jour à prendre en 2 fois	Circulaire FP/4 n°1864 du 9 août 1995	Demande	Mesure de bienveillance relevant de l'appréciation du chef de service. L'autorisation peut être accordée si l'administration possède une organisation matérielle appropriée à la garde de l'enfant ou si l'enfant se trouve proche du lieu de travail
Aménagement des horaires de travail pour les femmes enceintes	A partir du 3ème mois de grossesse, allègement d'1 heure sur l'horaire journalier (pas de cumul possible), ces heures n'étant pas récupérables	Circulaire FP/4 n°1864 du 9 août 1995	Sur avis du médecin chargé de la prévention au vu des pièces justificatives	Mesure de bienveillance relevant de l'appréciation du chef de service. Absences pouvant être accordées dans la mesure où elles sont compatibles avec le fonctionnement normal du service
Examens médicaux obligatoires antérieurs ou postérieurs à l'accouchement	Durée des examens	Directive n°92/85/CEE du 19 octobre 1992 Loi n°93-121 du 27 janvier 1993 Circulaire FP/4 n°1864 du 9 août 1995	Sur avis du médecin chargé de la prévention au vu des pièces justificatives ou sur certificat du médecin traitant	Autorisation d'absence de droit
Cohabitation avec une personne atteinte d'une maladie contagieuse	Variole : 18 jours Diphtérie et méningite cérébro-spinale : reprise du service après 2 examens médicaux bactériologiques négatifs effectués à 8 jours d'intervalle	Instruction n°7 du 23 mars 1950	Certificat médical	Mesure de bienveillance relevant de l'appréciation du chef de service. Le médecin assermenté de l'administration doit s'assurer que le fonctionnaire intéressé produit les justifications de prolongation d'absence ou remplit les conditions exigibles à son retour
Examens médicaux obligatoires liés à la surveillance médicale annuelle de prévention en faveur des agents	Durée des examens	Décret n°82-453 du 28 mai 1982	Sur avis du médecin chargé de la prévention	Autorisation d'asence de droit
POUR EXERCER CERTAINES FONCTIONS				
Agents de l'Etat représentants des parents d'élèves dans les cas suivants : - réunions de parents d'élèves et de conseils d'écoles (maternelles et élémentaires) - réunions de conseils d'établissements (collèges et lycées)	Durée des réunions	Circulaire n°1913 du 17 octobre 1997	Convocation	Mesure de bienveillance relevant de l'appréciation du chef de service. Aménagement d'horaire accordé de manière ponctuelle par les chefs de service

ANNEXE N°5 : AUTORISATIONS D'ABSENCE

MOTIF	DUREE	TEXTES DE REFERENCE	JUSTIFICATIFS	COMMENTAIRES
Agents de l'Etat sapeurs-pompiers volontaires	Durée des missions opérationnelles et des actions de formation intervenant pendant le temps de travail	Loi n°96-370 du 3 mai 1996 Circulaire du 19 avril 1999	Tout justificatif	Absences accordées par les chefs de service dans la mesure où elles sont compatibles avec le fonctionnement normal du service
Participation à un jury de la cour d'assises	Autorisation spéciale d'absence de droit pour la durée du procès	Articles 258, 267 et 288 du code de procédure pénale Lettre FP/7 n°6400 du 2 septembre 1991	Convocation	Autorisation d'absence obligatoire sous peine d'amende pour l'intéressé
Activités syndicales : **- participation aux réunions syndicales** **- participation aux travaux des organismes professionnels** **- participation aux réunions organisées par l'administration (CAPA, CHS, ...)** **- participation au choix de l'agent à une des réunions d'information syndicale**	Autorisation d'absence de : - 1 heure par mois pour les réunions syndicales - 10 jours par an pour la participation aux travaux des organismes professionnels - Délai de route + durée de la réunion + temps égal à la durée prévisible de la réuion destiné à sa préparation pour les réunions organisées par l'administration - 1 heure mensuelle d'information syndicale	Décret n°82-447 du 28 mai 1982 relatif à l'exercice du droit syndical dans la fonction publique Circulaire FP n°1487 du 18 novembre 1982	Convocation	Autorisations d'absence de droit, accordées par les chefs de service dans la mesure où elles sont compatibles avec le fonctionnement normal du service
Agents de l'Etat candidats à une fonction publique élective	Facilités de service pour participer aux campagnes électorales de : - 20 jours maximum pour les élections présidentielles, législatives, sénatoriales et européennes - 10 jours maximum pour les élections régionales, cantonales ou municipales	Circulaire FP/3 n°1918 du 10 février 1998 Loi n°2002-276 du 27 février 2002 Circulaire FP/3 du 18 janvier 2005	Tout justificatif	Mesure de bienveillance relevant de l'appréciation du chef de service. Facilités de service dont la durée est ensuite imputée sur les congés annuels ou, lorsque cela n'est pas possible, reportée sur une autre période
Agents de l'Etat titulaires de fonctions électives : **- participation aux sessions des assemblées dont ils font partie** **- exercice de leur mandat d'élu local**	Autorisation d'absence : - durée des sessions des assemblées dont ils font partie - crédit d'heures forfaitaires par trimestre selon le mandat (réduit au prorata si travail à temps partiel); pour les fonctionnaires occupant des fonctions municipales, la durée de l'autorisation d'absence est au maximum égale à la durée totale des sessions. Dans la mesure où les nécessités de service le permettront, les autorisations spéciales d'absence pourront être accordées en dehors des sessions dans les limites suivantes : 1 journée ou 2 demi-journées / semaine pour les maires des communes de 20 000 habitants au moins, et 1 journée ou 2 demi-journées / mois pour les maires des autres communes et adjoints de communes de 20 000 habitants au moins.	Instruction n°7 du 23 mars 1950 code général des collectivités territoriales	Demande formulée au chef de service : - 24h avant pour la participation aux sessions des assemblées - 72h avant l'exercice du mandat d'élu	Autorisation d'absence de droit. Pour l'exercice du mandat d'élu local, les heures non utilisées pendant un trimestre ne sonrt pas reportables

CONSIGNES GENERALES DE SECURITE
UNIVERSITE BLAISE PASCAL

ACCIDENT:

➢ En cas d'urgence, appelez le SAMU ☎: **15**
Pour le campus des Cézeaux, faites le 42 (puis l'infirmerie du site):

➢ Infirmerie ☎: **70.22 (Cézeaux)**, ☎: **66.00 (Gergovia)**, ☎: **20.12 (IUT)**
➢ Prévenez le secouriste le plus proche

BRULURE CHIMIQUE OU THERMIQUE:

➢ Dans tous les cas, lavez abondamment à l'eau pendant 15 minutes
➢ En cas de brûlure cutanée par l'acide fluorhydrique, après lavage appliquez immédiatement le gel de gluconate de calcium mis à votre disposition
➢ Dans tous les cas, consultez immédiatement l'infirmerie, ou en cas d'absence faites le ☎: **15 ou 42** (campus des Cézeaux)

INCENDIE:

➢ Attaquez le feu au moyen d'extincteurs appropriés sans prendre de risques
➢ Brisez la vitre du boîtier d'alarme situé dans le couloir (boîtier rouge)
➢ Donnez l'alerte ☎: **18 ou 42** (campus des Cézeaux)
➢ En cas d'évacuation, suivez les instructions du guide d'évacuation et regroupez-vous vers les zones de rassemblement prévues pour votre bâtiment
➢ Dans la fumée, baissez-vous, l'air frais est près du sol
➢ Ne revenez jamais en arrière sauf sur ordre du guide d'évacuation
➢ N'utilisez pas les ascenseurs pour évacuer

INTERDICTION DE FUMER:

➢ Il est strictement interdit de fumer dans les locaux et à l'intérieur des bâtiments (Décret du 15 novembre 2006)

CIRCULATION ET STATIONNEMENT:

➢ Respectez les limitations de vitesse et le code de la route
➢ Respectez les parkings prévus à cet effet
➢ Ne bloquez pas les accès des véhicules de secours

INSTALLATIONS ELECTRIQUES:

➢ Toute intervention doit être réalisée par un personnel formé et **habilité**
➢ Il est strictement interdit d'intervenir sur une installation électrique **sous tension**
➢ Les travaux sur ces installations ne peuvent être réalisés que par du personnel des services techniques de l'Université ou par une entreprise extérieure spécialisée et mandatée
➢ Toute consignation d'une installation électrique se fera sous contrôle d'une personne habilitée des services techniques de l'Université

PROCEDURE DE PERMIS DE FEU:

➢ Il est interdit de faire des travaux par points chauds (travaux avec présence de flammes ou étincelles) sans avoir préalablement établi un permis de feu
➢ Pour toute demande, contactez le service technique de l'Université ☎: **61.62** ou **61.60**

FUITE D'EAU:

➢ En cas de fuite d'eau, **NE COUPEZ PAS L'ALIMENTATION GENERALE** sans avoir consulté les utilisateurs, l'ACMO ou l'ingénieur Hygiène et Sécurité (certaines manipulations nécessitent une alimentation permanente en eau pour des raisons de sécurité)
➢ Avant de remettre en marche, prévenez les utilisateurs

FUITE DE GAZ:

➢ Fermez si possible la vanne d'alimentation en amont de la fuite

➢ Prévenez immédiatement les utilisateurs ainsi que les services techniques ☎: **61.62** ou **61.60**
➢ Arrêtez toutes les manipulations ou appareillages susceptibles d'engendrer un risque d'incendie et / ou d'explosion

Si nécessaire:

↳ **FAITES EVACUER** la zone concernée
↳ Appelez les secours ☎: **18 ou 42** (campus des Cézeaux)

AVANT DE REMETTRE EN MARCHE, INFORMEZ LES UTILISATEURS

ANNEXE N°7 : 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 8 – PERSONNES RESSOURCES EN MATIERE DE SECURITE ET DE PREVENTION DES RISQUES

- **Assistants de prévention** :

M.Nicolas CLUZEL, 04.73.34.67.43

M.Mhammed BENBAKKAR, 04.73.34.67.47, spécialisé dans les risques chimiques.

- **Equipiers de sécurité incendie** :

- Equipiers de 1ere intervention
  - 1 à 2 noms
- Chargés d'évacuation (guide file, serre file)
  - Guide file :
  - Serre file :

- **Personnes compétentes dans un domaine de gestion du risque**

Personne en charge de la radioactivité : M.Pierre-Jean GAUTHIER, 04.73.34.67.26

Référent sécurité laser : M.Franck POINTUD, 04.73.34.67.56

Personne en charge de la sécurité des systèmes d'information : (article 13) : M. Philippe Cacault est le CSSI de l'unité.

- **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).

Dr Laurette ROCHER 04 72 69 26 76, Médecin de prévention (personnel CNRS)

Dr M.C. RATINAUD, Médecin de prévention (personnel Université)

ANNEXE N°9 : 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°10 : Charte Informatique

Charte Utilisateur pour l'usage des ressources informatiques et des services Internet de l'Observatoire de Physique du Globe de Clermont Ferrand

Les différentes composantes de l'UFR OPGC sont: l'Observatoire de Physique du Globe (UMS 833), le Laboratoire Associé de Météorologie Physique (UMR 6016) et le Laboratoire Magmas et Volcans (UMR 6524). Leurs personnels sont donc soumis aux règles prévues par cette Charte.

Ce texte est avant tout un code de bonne conduite. Il a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation afin d'instaurer un usage correct des ressources informatiques et des services Internet, avec des règles minimales de courtoisie et de respect d'autrui.

1. Définitions

- On désignera de façon générale sous le terme "ressources informatiques" les moyens informatiques de calcul , de stockage, de gestion locaux, d'utilisation de la bande passante, ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par l'OPGC.
- On désignera par "services Internet" la mise à disposition par des serveurs locaux ou distants de moyens d'échanges, de publication ou de diffusion d'informations diverses : Web, messagerie, forum, ftp, bases de données,...
- On désignera sous le terme "utilisateur" les personnes ayant accès ou utilisant les ressources informatiques et services Internet.

2. Accès aux ressources informatiques et services Internet

Les utilisateurs peuvent accéder aux ressources informatiques et aux services Internet de l'OPGC uniquement dans le cadre de leur activité professionnelle, et après signature de la présente charte.

L'activité professionnelle est celle prévue par les statuts du GIP RENATER auquel est lié le CNRS et l'Université, à savoir: les activités de recherches, d'enseignements, de développements techniques, de transferts de technologies, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentations de nouveaux services présentant un caractère d'innovation technique, mais également toute activité administrative et de gestion découlant ou accompagnant ces activités.

L'utilisation des ressources informatiques partagées de l'OPGC et la connexion d'un équipement sur le réseau sont en outre soumises à autorisation. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Ces autorisations peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée. L'OPGC pourra en outre prévoir des conditions d'accès spécifiques à son organisation : d'authentification par carte à puce, certificat numérique, filtrage d'accès sécurisé ...
En aucun cas les utilisateurs ne doivent connectés des équipements personnels privés.

3. Règles d'utilisation, de sécurité et de bon usage

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et aussi à celle de l'OPGC.

L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.

En particulier, tout utilisateur:

- doit appliquer les recommandations de sécurité de l'OPGC;
- doit assurer la protection de ses informations et il est responsable des droits qu'il donne

aux autres utilisateurs; il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition;

- doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater dans les communications ou le comportement de son système;
- doit suivre les règles en vigueur au sein de l'OPGC pour toute installation de logiciel, à savoir s'assurer de la bonne provenance et de l'intégrité du logiciel, et appliquer systèmatiquement les mise à jour de sécurité;
- choisir des mots de passe sûrs (complexes, non basés sur un mot de dictionnaire, comportant des caractères non-alphanumériques et au minimum de 8 caractères), changés régulièrement, gardés secrets; en aucun cas il ne doit les communiquer à des tiers, et ni réutiliser un ancien mot de passe;
- s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage;
- ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité;
- ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement: en particulier, il ne doit pas modifier le ou les fichiers contenant des informations comptables ou d'identification;
- ne doit pas intercepter de communication entre tiers;
- ne doit pas quitter son poste de travail ni ceux en libre service sans se déconnecter en laissant des ressources ou services accessibles;
- Chaque utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. Il informe le service informatique de toute anomalie constatée dans le matériel.
- L'utilisateur doit s'efforcer de n'occuper que la quantité d'espace disque qui lui est strictement nécessaire et utiliser de façon optimale les moyens de compression des fichiers dont il dispose.
- Les activités risquant d'accaparer fortement les ressources informatiques (impression de gros documents, calculs importants, utilisation intensive du réseau, etc) devront être effectuées aux moments qui pénalisent le moins la communauté.

4. Conditions de confidentialité

La confidentialité des messages non chiffrés ne peut pas être garantie.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est pas destinataire ni directement, ni en copie. Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés, il devra auparavant en avoir fait la demande à la CNIL en concertation avec le Directeur de l'OPGC et la Direction des Contrats et des Affaires juridiques du CNRS et en avoir reçu l'autorisation. Il est rappelé que cette autorisation n'est valable que pour le *traitement* défini dans la demande et pas pour le *fichier* lui-même.

5. Respect de la législation concernant les logiciels

Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle. Ces dernières ne peuvent être effectuées que par la personne habilitée à cette fin par le Directeur de l'OPGC.

Par ailleurs, l'utilisateur ne doit pas installer de logiciels à caractère ludique, ni contourner les restrictions d' utilisation d'un logiciel.

6. Préservation de l'intégrité des systèmes informatiques

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon

fonctionnement des systèmes informatiques et des réseaux, que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques.... Tout travail de recherche ou autre, risquant de conduire à la violation de la règle définie dans le paragraphe précédent, ne pourra être accompli qu'avec l'autorisation du responsable de l'entité et dans le strict respect des règles qui auront alors été définies.

7. Usage des services Internet (Web, messagerie, forum...)

L'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités professionnelles et dans le respect de principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur.

En particulier :

- il ne doit pas utiliser les ressources informatiques et les services Internet à des fins commerciales, personnelles autres que dans le cadre d'activités de formation, de culture ou de recherche, ou à des fins ludiques (jeux multimédia "en réseau", téléchargement de vidéos et musiques, ou autres);
- il ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables;
- il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède;
- il ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers;
- il ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur;
- il ne doit pas déposer des documents sur un serveur sauf si celui-ci le permet ou sans y être autorisé par les responsables habilités;
- il doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions...
- il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice au CNRS ou à l'Université,
- il doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire.

L'OPGC ne pourra être tenu pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé à ces règles.

8. Analyse et contrôle de l'utilisation des ressources

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau (connexions externes et internes) peuvent être analysés, contrôlés, et audités dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.

9. Rappel des principales lois françaises :

Il est rappelé que toute personne sur le sol français doit respecter la législation française en particulier dans le domaine de la sécurité informatique :

- 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 du 04/08/1994 relative à l'emploi de la langue française

- la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
- les dispositions du code de la propriété intellectuelle 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.

10. Application

La présente charte s'applique à l'ensemble des personnels de l'OPGC tous statuts confondus, et plus généralement à l'ensemble des personnes, permanentes ou temporaires, utilisant les moyens informatiques de l'Etablissement, ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir du réseau administré par l'OPGC.

Elle sera annexée, à titre d'information, aux contrats de travail conclus avec les agents contractuels qui auront accès au système informatique de leur unité.

Elle sera en outre signée par toute personne accueillie dans les différentes composantes de l'OPGC et ayant accès au système informatique de l'OPGC.

A Clermont Ferrand, le 17 Février 2015

Vu Patrick Bachelery Directeur de l'OPGC	Vu Joël Van Baelen Directeur du LaMP	Vu Pierre Schiano Directeur du LMV
	Joël VAN BAELEN Directeur du LaMP	Prof. P. SCHIANO Directeur UMR 6524

Nom: Prénom :

Date arrivée : Date départ :

Fonction : Responsable :

N°Bureau : Téléphone : 04 73 __ __ __

Signature :

ANNEXE N°11 : POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION OPERATIONNELLE DE L'UNITE

Politique de Sécurité des Systèmes d'Information (PSSI)

Document d'orientation de la sécurité des systèmes d'information du CNRS

Versions	Rédacteur	Autorité d'approbation	Date d'approbation
V1.0	Joseph ILLAND (FSD)	Arnold MIGUS (Directeur Général)	15 novembre 2006

Sommaire

Introduction : les enjeux de la PSSI

Partie I : Contexte et objectifs

1. Le contexte du CNRS
2. Le périmètre de la SSI au CNRS
3. Les besoins de sécurité
4. Les menaces et les impacts

Partie II : Principes d'organisation et de mise en œuvre

1. Organisation de la SSI au CNRS
2. Coordination avec les autres tutelles
3. Déclinaison d'une PSSI au sein d'une entité du CNRS
4. Principes de mise en œuvre de la PSSI

Introduction : les enjeux de la PSSI

Le haut potentiel de recherches du CNRS confère un caractère stratégique à **la protection de son patrimoine scientifique et technique**.

Les atteintes peuvent tout aussi bien toucher ses données scientifiques ou technologiques que ses outils ou moyens scientifiques, techniques et humains.

La **sécurité des systèmes d'information (SSI)** s'impose comme une composante essentielle de la protection du CNRS dans ses intérêts propres et dans ceux liés à des enjeux nationaux (intérêts fondamentaux de la nation).

Bien que cela soit difficile à évaluer, l'insécurité a un coût qui se manifeste lors d'incidents ou de dysfonctionnements.

Face aux risques encourus, et dans le contexte fonctionnel et organisationnel propre à l'organisme, il convient d'identifier ce qui doit être protégé, de quantifier l'enjeu correspondant, de formuler des objectifs de sécurité et d'identifier, arbitrer et mettre en œuvre les parades adaptées au juste niveau de sécurité retenu.

Cela passe prioritairement par la définition et la mise en place au sein du CNRS d'une « **Politique de Sécurité des Systèmes d'Information** » **(PSSI).**

La PSSI relève d'une vision stratégique de l'organisme et traduit un engagement fort de la direction générale. Elle s'inscrit nécessairement sur le long terme.

Elle est conforme aux dispositions législatives et réglementaires et cohérente avec les politiques et directives de niveau supérieur (ministérielles et interministérielles) ; elle se doit également d'être cohérente avec les politiques de sécurité des organismes partenaires.

Elle se déclinera ensuite :

- au niveau de l'organisme par un approfondissement du contexte (enjeux, menaces, besoins) et une explicitation des dispositions de mise en œuvre, au travers d'un Schéma Directeur de la SSI et/ou d'un plan d'action SSI
- au niveau des unités, par la définition d'une PSSI d'unité tenant compte des particularités propres à chaque unité et, pour ce qui est des unités mixtes, intégrant les orientations des autres tutelles.

(CAPSEC (Comment Adapter une Politique de Sécurité pour les Entités du CNRS) : méthodologie d'analyse de risques permettant à chaque unité de conduire une analyse de ses risques et de formuler des recommandations adaptées au contexte de l'unité).

Partie I : Contexte et objectifs

1) Le contexte du CNRS

Du fait de ses missions et de son organisation, le CNRS présente de nombreuses spécificités par rapport à d'autres entités (ministères, établissements publics, entreprises).

- **Le CNRS est le principal organisme national de recherche** avec 25 000 personnes directement rémunérées (dont 12 000 chercheurs) et un potentiel d'ensemble d'environ **60 000** personnes en englobant les personnels des unités mixtes.
- **La structure est très éclatée** : les unités propres de recherche du CNRS ainsi que les unités mixtes représentent plus de 1300 laboratoires implantés sur plusieurs centaines de sites.
- **L'organisation administrative s'appuie en région sur 19 délégations régionales.**
- **La structure est extrêmement ouverte**, située le plus souvent dans des campus où il est difficile de délimiter des zones à protéger
- Il s'agit d'une structure généralement **très imbriquée avec d'autres organismes**: le CNRS partage le plus souvent sa tutelle d'unités avec plusieurs organismes (universités, écoles d'ingénieurs, EPST, entreprises…) dont il faut intégrer la politique et les modes de fonctionnement ; par ailleurs le CNRS a rarement la maîtrise des infrastructures.
- **La diversité des activités de recherche** rend difficile des recommandations communes à des populations relevant de contextes professionnels très différents.
- **Les unités elles-mêmes sont très hétérogènes :** et il y a peu de similitude entre un grand laboratoire possédant des moyens financiers et humains importants, une culture et un savoir-faire en systèmes et réseaux et une petite unité de recherche qui a constitué son informatique par touches successives et sans personnel technique associé.
- **Le CNRS présente une forte dimension internationale**, avec plusieurs centaines d'accords de coopération internationale, 70 structures européennes et internationales, une dizaine de bureaux du CNRS implantés à l'étranger, plus de 40 000 missions annuelles à l'étranger, et l'accueil dans les unités d'environ **15 000 étudiants et chercheurs étrangers**, à titre permanent ou à titre de visites ou stages.
- **L'état d'esprit des chercheurs est par nature ouvert** et non naturellement enclin au respect de dispositions de sécurité contraignantes.
- **Le CNRS présente une sensibilité importante au regard de la protection du patrimoine scientifique et technique,** liée aux enjeux et liens de certaines recherches avec la défense ou aux risques de prolifération, ou plus souvent encore du fait de l'intérêt industriel et économique des retombées technologiques. La moitié des laboratoires est repérée comme « sensible » et 150 unités sont classées « Etablissements à Régime Restrictif (ERR)».
- **La typologie des données à protéger est très variée** (données scientifiques, techniques ou de gestion de sensibilité très variable).

- **Les moyens financiers et humains** ne sont pas toujours adaptés à la mise en œuvre nécessaire des recommandations en matière de gestion de la sécurité et d'acquisition d'outils de protection.

En contrepartie le CNRS dispose d'atouts propres liés à la qualité et la compétence des personnels dans le domaine de l'informatique et des réseaux. S'y ajoutent un sens de l'initiative et un esprit d'équipe qui facilitent les relations et le fonctionnement en réseaux.

Le contexte législatif et réglementaire :

La mise en œuvre de systèmes d'information est soumise à des obligations relevant de nombreux textes d'ordre législatif et réglementaire qui confèrent un enjeu juridique important à cette activité.

On peut citer en particulier la loi sur la confiance en l'économie numérique (LCEN), la loi relative à l'informatique et aux libertés (loi CNIL), la loi relative à la fraude informatique (loi Godfrain), les instructions et recommandations interministérielles provenant du Secrétariat Général de la Défense Nationale (SGDN).

S'y ajoutent des dispositions relevant du code de la propriété industrielle, et des dispositions pénales (en particulier articles 226 et 227).

La sécurité des systèmes d'information fait par ailleurs l'objet d'une normalisation (norme ISO 27001).

Le corpus correspondant ainsi que le suivi de la jurisprudence font l'objet de documents de diffusion interne.

2) Le périmètre de la SSI au CNRS

La sécurité des systèmes d'information du CNRS doit nécessairement couvrir l'ensemble des systèmes d'information de l'organisme avec toute la diversité que cela implique dans les usages, les lieux d'utilisation, les méthodes d'accès, les personnes concernées. C'est ainsi que l'existence d'implantations à l'étranger et l'importance des missions extérieures lui confère également une dimension internationale.

Le périmètre de la SSI est donc très large.

Ce périmètre englobe les trois ensembles de systèmes d'information interconnectés par le réseau RENATER :

- le système d'informatique de gestion géré par la DSI et les délégations régionales
- les systèmes d'information des unités (bureautique, applications scientifiques, stockage, traitement et interprétation de données, applications INTERNET (dont sites Web institutionnels), messagerie…)
- quelques centres importants de ressources (calcul, données…).

Il inclut les unités mixtes dépendant du CNRS et d'autres tutelles. L'infrastructure étant en de nombreux endroits partagée avec d'autres organismes (universités, …), du personnel non CNRS est amené à travailler sur les systèmes d'information du CNRS.

Sont également à prendre en compte, dans le périmètre de la SSI, les équipements de l'entité ou ceux gérés par le service informatique d'une tutelle, sur lesquels s'exécutent les fonctions essentielles comme la communication (serveur de messagerie, machines internes cibles de connexion depuis l'extérieur), la gestion financière et comptable (serveur XLAB), la modélisation (serveur de calcul), la publication (serveur web, serveur d'impression), le stockage, le traitement et l'interprétation des données (serveur de fichiers, pilotage/contrôle de manipulations). Par ailleurs, du fait de l'évolution des technologies, certains systèmes (téléphonie, visioconférence, photocopieur, vidéosurveillance), traditionnellement en dehors du champ de l'informatique, font désormais partie du périmètre.

La SSI du CNRS intègre également les prestations externes telles que l'hébergement de serveurs et la sous-traitance dans leur incidence sur la sécurité interne des systèmes d'information.

Les usages liés à la mobilité (ordinateurs portables, connexions sans fil, assistants personnels, téléphones portables…) sont également à prendre en compte du fait que ces usages se pratiquent généralement en milieu non protégé.

L'utilisation d'un moyen informatique privé ou extérieur fait entrer l'équipement dans les ressources informatiques de l'unité et comme tel dans le périmètre de la SSI.

Toutefois ne sont pas compris dans ce périmètre les unités ayant des liens forts avec le CNRS (intégrant des équipes CNRS mises à disposition ou bénéficiant de financements…) mais échappant à sa tutelle.

3) Les besoins de sécurité

Il s'agit de protéger l'outil de travail (disponibilité), les données (confidentialité, disponibilité, intégrité), le personnel des unités et l'organisme.

Les critères de sécurité

La sécurité du Système d'Information repose sur trois critères :

- Confidentialité : « La confidentialité est la propriété qu'une information n'est ni disponible ni divulguée aux personnes, entités ou processus non autorisés » norme ISO 7498-2 (ISO90).
- Disponibilité : Propriété d'accessibilité au moment voulu des données et des fonctions par les utilisateurs autorisés.
- Intégrité : « L'intégrité est la prévention d'une modification non autorisée de l'information » norme ISO 7498-2 (ISO90).

Ces critères peuvent être quantifiés selon une échelle de besoins de sécurité (cf. ci-après une évaluation issue des travaux du groupe CAPSEC).

Confidentialité	Disponibilité	Intégrité
Perte de confidentialité sans conséquence	Délai supérieur à une semaine	Perte d'intégrité sans conséquence
Le sinistre ne risque pas de provoquer une gêne notable dans le fonctionnement ou les capacités de l'organisme. Ex : données publiques, visibles par tous.	Des services qui apportent un confort supplémentaire mais pas indispensable.	Le sinistre ne risque pas de provoquer une gêne notable dans le fonctionnement ou les capacités de l'organisme. Ex : aucune vérification.
Perte de confidentialité entraînant des gênes de fonctionnement	Délai > 8 heures et <= 1 semaine	Perte d'intégrité entraînant des gênes de fonctionnement
Susceptible de provoquer une diminution des capacités de l'organisme. Ex : données liées aux compétences ou savoir-faire internes, dans un contexte de groupe de confiance, dont vous protégez toutes les traces écrites.	Ressources pour lesquelles il existe une alternative. Ex : imprimantes.	Susceptible de provoquer une diminution des capacités de l'organisme. Ex : vérification des données, sans validation : des fautes d'orthographe sur une page web nuisent à l'image de marque du laboratoire
Perte de confidentialité entraînant des conséquences dommageables	Délai > 2heures et <= 8 heures	Perte d'intégrité entraînant des conséquences dommageables
Susceptible d'amoindrir les capacités de l'organisme, avec des conséquences telles que des pertes financières, sanctions administratives ou réorganisation Ex : données liées à un engagement de confidentialité dans un contrat.	Sans conséquence vitale humainement Ex : arrêt du réseau, de la messagerie, données vitales non disponibles...	Susceptible d'amoindrir les capacités de l'organisme, avec des conséquences telles que des pertes financières, sanctions administratives ou réorganisation Ex : données qui sont validées et contrôlées par des moyens techniques ou humains.
Perte de confidentialité entraînant des conséquences graves	Délai : entre temps réel et <= 2 heures	Perte d'intégrité entraînant des conséquences graves
Susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants, la restructuration de l'organisme, des pertes financières. Ex : données secret défense.	Ressources qui mettent en péril la vie (humaine ou animale ou biologique). Ex : expériences biologiques ou physiques pilotées automatiquement, système de sécurité.	Susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants, la restructuration de l'organisme, des pertes financières. Ex : données avec au moins deux niveaux de validation et de contrôle différents (techniques ou humains).

Les besoins de sécurité

Protection de l'outil de travail : les postes informatiques, les réseaux, les applications et les données, constituent « le Système d'Information » du CNRS. Cet ensemble est indispensable à la fois pour les activités nécessaires à la recherche, mais aussi pour la gestion des entités. La disponibilité et l'intégrité de cet outil doivent donc impérativement être placées à l'abri de menaces internes ou externes.

Protection des données : dans quelques cas il peut s'agir de « données classifiées de défense », mais le plus souvent il s'agit de « données sensibles » telles que :

- Les données scientifiques : liées à des contrats industriels, à un savoir-faire interne, expérimentales, liées à des coopérations nationales ou internationales, scientifiques, techniques, économiques, liées à la valorisation de la recherche, liées au centre de documentation, téléphoniques et de visioconférences
- Les données de gestion : authentification, gestion comptable et financière, gestion des ressources humaines, documents contractuels
- Les données nominatives : liées à la vie privée des personnes, liées à l'enseignement
- Les données stratégiques : informations d'ordre politique ou stratégique ou touchant des questions de défense, informations sécurité…

La protection des données sensibles suppose l'identification préalable de ces données, la détermination du type de protection nécessaire (confidentialité, disponibilité, intégrité) et l'évaluation de leur degré de sensibilité (quantification des besoins de sécurité).

La sensibilité des données est appréciée lors d'un inventaire au cours duquel des questions touchant à « la vie de la donnée » doivent être posées :

- Quel est son type ?
- Où réside t-elle ?
- Par qui est-elle partagée (« besoin d'en connaître ») ?
- Quelle(s) menace(s) est-elle susceptible de subir ?

Protection juridique : la mise en œuvre des systèmes d'information s'inscrit dans un cadre législatif et réglementaire destiné en particulier à protéger les droits de propriété intellectuelle et industrielle et ceux de la vie privée (fichiers nominatifs, cybersurveillance…). Dans ce cadre, la responsabilité administrative et pénale de la hiérarchie et des administrateurs systèmes et réseaux peut être recherchée.

4) Les menaces et les impacts

Les menaces

La mise à exécution de menaces volontaires ou involontaires, humaines ou matérielles peut porter atteinte au SI, aux personnels et à l'organisme. Il convient de distinguer ce qui relève **d'attaques délibérées (agressions)** et ce qui relève de **sinistres naturels** (incendie, explosion, inondations…).

Dans le cadre d'une étude de risques, il est possible de considérer les menaces comme la méthode EBIOS (*) le préconise, c'est-à-dire inventorier les menaces en considérant la probabilité que la menace devienne réalité ; la menace est prise en compte en fonction des critères suivants :

- Type d'élément menaçant : environnemental ou humain ou naturel
- Cause d'élément menaçant : délibérée ou accidentelle
- Potentiel d'attaque : opportunités ou ressources limitées, accidentel et aléatoire, haut degré d'expertise d'opportunité et de ressources

(*) EBIOS : *« Expression des Besoins et Identification des Objectifs de Sécurité »* : démarche d'analyse de sécurité élaborée par la Direction Centrale de la Sécurité des Systèmes d'Information du SGDN.

Un référentiel des menaces est disponible dans EBIOS. Il a été repris et adapté pour le CNRS dans le cadre des travaux du groupe CAPSEC.

Les Impacts

Les impacts des attaques sur les critères de sécurité peuvent se traduire ainsi :

Critères	Attaques	Impacts
confidentialité	**Divulgation, accès** par des tiers non autorisés et **détournement** à des fins délictueuses, de données confidentielles (touchant des travaux confidentiels, des données scientifiques ou technologiques, des données personnelles telles que médicales ou financières…), que ces données soient stockées ou échangées (messagerie)	Pertes du patrimoine scientifique ; pertes d'avance technologique et technique ; pertes financières ; contentieux juridique
disponibilité	**Vol de matériel**, **émission de malware** (virus, ver, déni de service…) **Sinistres**	Interruption de service ; paralysie ou désorganisation conduisant à l'incapacité opérationnelle de fonctionnement, de décision, de gestion, de sécurisation ; saturation de ressources, de systèmes d'alerte ; perte de données précieuses (scientifiques ou de gestion) par absence ou insuffisance de sauvegarde ; atteinte à la sécurité du personnel, des usagers ; perte d'image de marque
intégrité	**Modification accidentelle ou délibérée** (défiguration de sites Web…), **piégeage** de systèmes d'information, **émission de malware** (bombes logiques, chevaux de Troie, sniffeurs…), **vol** ou **détournement** de moyens informatiques à des fins délictueuses (compromission de serveurs…)	Résultats de fonction incomplets ou incorrects ; expérimentations non crédibles ; prises de décisions inadaptées ; appropriation frauduleuse de biens ; prise de contrôle d'un système physique ; perte du patrimoine scientifique ; perte d'image de marque ; atteinte à des libertés individuelles (cybersurveillance indue…)

À partir des menaces retenues, il convient d'évaluer les risques pour chacune d'entre elles (probabilité d'occurrence et mesure des conséquences).

Les parades viseront donc à peser sur ces deux facteurs : réduire la probabilité d'occurrence, atténuer l'impact en cas de réalisation effective de la menace.

Inversement des éléments tels que la négligence, l'insuffisance de formation ou d'information, les insuffisances de management de la sécurité, l'absence de consignes claires… sont des facteurs aggravants du risque, en amplifiant la probabilité d'occurrence de la menace ou la conséquence de l'incident survenu. En conséquence il est nécessaire de procéder à une analyse de risques.

Partie II : Principes d'organisation et de mise en œuvre

1) Organisation de la SSI au CNRS

Pilotage

Au sein du CNRS, la responsabilité générale de la sécurité des systèmes d'information relève du directeur général du CNRS en tant qu'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI) du CNRS. Il est assisté dans cette fonction par le Fonctionnaire de Sécurité de Défense (FSD), également Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) du CNRS.

Le pilotage stratégique est assuré de manière concertée par un comité de pilotage de la SSI présidé par une personnalité reconnue dans ce domaine et nommée par le directeur général du CNRS. Sont en particulier membres de ce comité, le FSD, le chargé de mission SSI, les directeurs de la DSI et de l'UREC, le secrétaire général du CNRS ou son représentant, un représentant de la DAJ, un représentant du département scientifique compétent, un représentant du HFD du ministère... Ce comité définit les grandes orientations de la SSI, validées par le directeur général du CNRS.

Par délégation du directeur général, le pilotage courant est de la responsabilité du FSD en concertation avec l'UREC au sein de laquelle est identifié un « chargé de mission SSI », fonctionnellement rattaché au FSD au titre de cette mission.

La mise en œuvre opérationnelle est assurée par l'UREC, qui gère la chaîne fonctionnelle et assure la conduite des différents projets et études techniques dans ce domaine. Pour cette dernière mission l'UREC s'appuie sur un réseau d'experts oeuvrant au niveau national ainsi que sur le réseau des coordinateurs régionaux.

La politique de sécurité des systèmes d'information du CNRS s'inscrit dans le cadre de la politique et des directives émanant de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), en charge de la sécurité des systèmes d'information au niveau national. Cette politique et ces directives sont relayées, pour ce qui est de la recherche, par le Haut Fonctionnaire de Défense du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche et par le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) placé auprès de lui.

Pour la définition et la mise en œuvre de la politique de sécurité des systèmes d'information, une concertation étroite est donc menée avec la DCSSI et le service du HFD, ainsi qu'avec les autres partenaires que sont les universités, les autres organismes de recherche et le réseau RENATER.

Mise en œuvre

Chaîne organique et fonctionnelle au CNRS en matière de SSI

Chaîne organique

L'application des dispositions de protection des systèmes d'information relève de la responsabilité de la **chaîne organique** (direction générale du CNRS, départements scientifiques, délégations régionales, directions d'unités de recherche ou de services) avec l'accompagnement des entités spécialisées (DSI, pour ce qui est des systèmes d'information de gestion du CNRS, UREC pour ce qui est des réseaux et de leurs applications).

Les responsables hiérarchiques d'unités (directeurs d'unités de recherche, délégués régionaux pour ce qui est de leur délégation) sont responsables de la sécurité des systèmes d'information de leur unité.

Pour assurer cette fonction, ils disposent de l'appui de la chaîne fonctionnelle SSI du CNRS (et le cas échéant de celle d'autres tutelles) et des moyens internes spécialisés (qu'ils ont la charge de définir : désignation au sein de leur unité d'un chargé de la SSI – cf ci-après-)

Outre leur responsabilité hiérarchique interne sur les services de leur délégation, les délégués régionaux ont la responsabilité de la coordination des directeurs d'unité en matière de SSI, en particulier en ce qui concerne l'application des réglementations, directives et consignes relevant de la SSI, la bonne adéquation des moyens en liaison avec les autres partenaires institutionnels, l'application des plans de prévention et d'intervention, la gestion des incidents, les relations avec les autres tutelles.

Ils ont, au titre de ce rôle, autorité sur la coordination régionale de la SSI (CRSSI) qui relève de la chaîne fonctionnelle spécialisée de la SSI.

Chaîne fonctionnelle spécialisée de la SSI

Pour conduire la politique de sécurité des systèmes d'information et faciliter sa mise en œuvre, le CNRS, sous l'autorité du directeur général en tant qu'AQSSI, s'appuie sur une chaîne fonctionnelle interne spécialisée en SSI qui s'inscrit elle-même dans la chaîne fonctionnelle nationale animée par la Direction Centrale de la Sécurité des Systèmes d'Information (SGDN/DCSSI).

La chaîne fonctionnelle SSI du CNRS est composée comme suit :

Au niveau national

- des structures de pilotage définies ci-dessus (FSD, UREC et comité de pilotage stratégique de la SSI)
- de Responsables de la Sécurité des Systèmes d'Information (RSSI) de structures nationales, lorsque des moyens ou des thématiques nécessitent une approche coordonnée au niveau national au profit de plusieurs entités, sous la responsabilité de ces structures nationales. C'est en particulier le cas pour la DSI compte tenu de son implication nationale en tant que chargée des

applications de gestion et des systèmes d'information des délégations et en tant que gestionnaire des procédures de déclaration à la CNIL.

- d'experts SSI susceptibles d'être sollicités au niveau national sur des travaux permanents ou ponctuels en appui du travail technique et d'animation nationale de l'UREC.

Au niveau régional

- d'une coordination régionale de la SSI (**CRSSI**) oeuvrant selon les directives techniques (de métier) du FSD et de l'UREC et sous la responsabilité du délégué régional pour ce qui est de la mise en œuvre des actions de coordination régionale relevant des compétences des délégués ; cette CRSSI a en particulier pour missions :
  - le suivi de l'état de sécurité des unités du périmètre de la délégation régionale (documents de PSSI, identification du Chargé de la SSI dans l'unité, bilans de sécurité, appréciation des besoins…),
  - le suivi de la mise en œuvre des dispositions de SSI définies au niveau national, remontées des dysfonctionnements vers l'UREC voire le FSD,
  - les contacts avec les Responsables de la Sécurité des Systèmes d'Information d'autres tutelles,
  - la conduite d'actions de formation et d'information et d'actions de conseil et soutien à destination des Chargés de la SSI dans les unités (animation du réseau),
  - la conduite d'actions d'information et de sensibilisation des unités,
  - le conseil et soutien aux chargés de SSI des unités, en cas d'incident,
  - le relais d'information entre les chargés de SSI des unités, l'UREC et le FSD, au titre de la chaîne fonctionnelle SSI,
  - la participation aux exercices d'alerte et à la gestion de crise,
  - la participation en tant que de besoin et selon le degré d'expertise individuelle à des travaux menés au niveau national (groupes de travail, réunions de coordinations, actions de formation),
  - le suivi d'un tableau de bord régional SSI et la rédaction du bilan annuel régional.

Cette coordination régionale peut être assurée de manière collégiale, par une équipe de quelques personnes missionnées à cet effet, experts en SSI, associant dans la mesure du possible un expert SSI de la délégation et un ou plusieurs experts SSI d'unité de recherche locales.

Les conditions d'exercice (à temps partiel) de ces missions doivent être formalisées (missions affichées au titre de leur poste, conditions de déplacements liées à ces missions SSI….).

L'organisation de cette coordination régionale est arrêtée localement en concertation entre le FSD, l'UREC et le délégué régional.

Au niveau local

- des Chargés de la Sécurité des Systèmes d'Information (CSSI), spécialistes des systèmes d'information, et dont la mission est d'assister les directeurs d'unité dans l'exercice de leur responsabilité en matière de SSI.

Pour chaque unité doit être identifié un CSSI désigné par le directeur de l'unité. Dans le cas de structures légères ou relevant d'autres tutelles ou dans le cas d'unités partageant les mêmes infrastructures, le CSSI peut ne pas appartenir à l'unité, la fonction étant alors mutualisée.

L'identification d'un CSSI dans les unités classées ERR (Etablissements à Régime Restrictif) est prioritaire.

A défaut d'identification d'un CSSI spécifique, en interne ou en externe, le rôle est directement assuré par le directeur de l'unité.

Dans le cas d'unités mixtes, les dispositions contractuelles entre tutelles peuvent prévoir le mode d'exercice des responsabilités de SSI et en particulier la prise en charge par l'une des tutelles de tout ou partie de la responsabilité en matière de SSI. Le CSSI de l'unité relève alors de la chaîne fonctionnelle de cette tutelle, tout en gardant un lien de coordination avec les autres tutelles.

Sous l'autorité du directeur d'unité, le CSSI a en particulier pour missions de :

- promouvoir la mise en place d'une PSSI d'unité,
- veiller à la mise en place des mesures de sécurité nécessaires,
- veiller à l'application des instructions et recommandations,
- veiller à la bonne exploitation des avis des CERT RENATER et CERTA,
- sensibiliser les utilisateurs,
- prendre les bonnes mesures en cas d'incident (ou s'assurer qu'elles sont prises),
- veiller à la prise en compte de la sécurité dans la rédaction des contrats de sous-traitance et les cahiers des charges des applications,
- veiller au respect des formalités requises par la loi Informatique et Libertés pour les traitements de données à caractère personnel,
- assurer la veille en matière de SSI et les niveaux relationnels nécessaires en liaison avec la coordination générale et plus généralement la chaîne fonctionnelle SSI.

Selon l'importance et la structuration de l'unité, le CSSI peut être secondé dans ces fonctions par d'autres personnes de l'unité. La ventilation des tâches doit alors être précisée.

Il est important que les fonctions de CSSI soient officialisées et reconnues tant en interne qu'à l'extérieur de l'unité.

2) Coordination avec les autres tutelles

Principe général

L'application de la politique de sécurité des systèmes d'information doit tenir compte de la situation des unités et de l'éventuel partage de tutelle avec d'autres organismes.

Le directeur de l'unité a la charge d'arrêter la politique de SSI dans son unité. Celle-ci doit être conforme au document de politique générale de la SSI du CNRS, mais les règles d'application peuvent différer en fonction des consignes propres à la tutelle responsable de la SSI.

Le système d'information de l'unité fait partie du SI du CNRS. La PSSI interne adoptée satisfera notamment les points suivants :

- la préservation des accès au système d'information du CNRS (administration, gestion...)
- l'articulation interne au CNRS des responsabilités organiques et fonctionnelles en matière de SSI et en particulier la responsabilité du directeur d'unité.

Dans le cas des unités propres du CNRS, les dispositions organisationnelles telles que décrites supra s'appliquent et relèvent de la seule responsabilité du CNRS.
Lorsque ces unités sont soutenues par d'autres organismes sur le plan informatique, la politique SSI de l'unité demeure de la responsabilité du CNRS tout en tenant compte des contraintes locales de l'organisme hébergeur.

Dans le cas d'unités mixtes, les dispositions contractuelles qui régissent la tutelle de l'unité (contrat quadriennal) incluent celles relatives à la sécurité des systèmes d'information en définissant en particulier les responsabilités respectives. Ce document définit la PSSI de référence pour l'unité mixte. En tant que responsable de la SSI de son laboratoire, le directeur de l'unité :

- s'assure que les documents de PSSI de son unité (charte, gestion des traces…) sont en accord avec ceux de toutes ses tutelles (CNRS, EPST, universités...)
- désigne le CSSI de son unité, celui-ci étant le « correspondant sécurité » pour les autres tutelles. Ce CSSI fait partie des chaînes fonctionnelles de chaque tutelle et assure les liens d'information correspondants. Le CSSI de l'unité doit en particulier disposer de la part de ces tutelles de toutes les informations nécessaires à l'exercice de son activité.

En cas d'incident

Les incidents informatiques doivent remonter par la voie fonctionnelle de la tutelle responsable, en assurant l'information des autres partenaires, avec si nécessaire une concertation sur les suites à donner telles que les dépôts de plainte.

En situation de crise grave survenant dans l'unité, il y a lieu d'informer la cellule de crise régionale et si nécessaire la cellule nationale. Inversement, l'unité mixte sera informée par la chaîne hiérarchique CNRS et par la chaîne fonctionnelle SSI du CNRS en cas d'événements graves justifiant le déclenchement d'alertes nationales. La mise en œuvre des plans de posture (VIGIPIRATE) ou d'intervention (PIRANET) est déclinée au sein de l'unité

par le directeur d'unité, les responsables informatiques et le RSSI d'unité. Cette mise en œuvre est pilotée et suivie par la tutelle SSI de l'unité.

En cas de litige

Les éventuelles divergences sont à traiter au niveau du CSSI de l'unité, de la coordination régionale, voire du délégué régional ; les éventuels arbitrages sont à soumettre à la voie fonctionnelle SSI (UREC et FSD et FSSI du ministère si nécessaire).

Principales tutelles : les universités et EPST

Une grande partie des unités mixtes partage leur tutelle avec des établissements de l'enseignement supérieur.

Une coordination nationale existe entre le service du FSD du CNRS, l'UREC, le service du HFD du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche, les pilotes des chaînes RSSI des universités (actuellement le CRU) et des chaînes FSD des universités, les RSSI des autres EPST, les CERTs (CERT-RENATER et CERTA).

Au niveau régional la coordination générale relève de la responsabilité du délégué régional ou de la CRSSI, par délégation. Les coordinateurs régionaux doivent pour leur part être en liaison avec les RSSI des universités et des EPST locaux et les FSD locaux.

En l'absence de dispositions contractuelles formelles, les présents principes de coordination doivent guider les relations entre le CNRS et les autres tutelles.

3) Déclinaison d'une PSSI au sein d'une entité du CNRS

Les unités doivent décliner à leur niveau la politique de sécurité des systèmes d'information de leur unité (PSSI d'unité)

Cette PSSI peut toutefois être commune à plusieurs unités relevant d'un cadre commun partageant les mêmes structures.

Inversement, dans le cas de structures importantes, l'élaboration de la PSSI de l'unité peut se faire selon des approches propres à des équipes internes lorsqu'elles disposent de systèmes d'information suffisamment distincts.

Une PSSI permet en effet à une entité (un laboratoire, une équipe de recherche ou un institut du CNRS, une direction, une délégation régionale…) d'avoir une approche méthodique et systématique pour garantir une sécurité homogène de son SI (Système d'Information).

À partir de documents, modèle générique et éléments de référence, l'entité définit sa propre PSSI adaptée à ses besoins.

Cette PSSI doit intégrer les politiques nationales de SSI des tutelles et en particulier celle de la tutelle principale en matière de SSI (si une telle tutelle est définie).

Une PSSI est également un document de dialogue entre les différents acteurs du SI (instances décisionnelles, responsables d'équipes de recherche ou de services, membres de l'entité, CSSI, Administrateurs Systèmes et Réseaux du service informatique s'ils sont distincts du CSSI, intervenants extérieurs, prestataires de services). Il est important que les personnels de l'entité participent au pilotage de la sécurité et donc ne la subissent pas.

À l'issue de ce dialogue, un consensus doit se dégager autour de la PSSI afin de définir une gestion cohérente des risques en fonction des moyens que l'entité peut ou doit investir dans la sécurisation de son SI.

Une fois validée en conseil de laboratoire, la PSSI permet d'une part de sensibiliser les membres du laboratoire à la sécurité du SI et de faire en sorte qu'ils s'approprient les éléments de sécurité, d'autre part de déterminer les solutions concrètes qui vont être mises en place au niveau de l'entité.

La PSSI d'une unité relève de l'initiative du directeur et du CSSI de l'unité.

Afin de faciliter la déclinaison d'une PSSI au sein de ses entités, le CNRS propose une méthodologie d'analyse de risques s'appuyant sur la méthode EBIOS de la DCSSI et développée dans le cadre des travaux du groupe CAPSEC.

4) Principes de mise en œuvre de la PSSI

La politique de sécurité des systèmes d'information du CNRS affiche un ensemble de principes d'ordre organisationnel et technique à caractère prioritaire. L'ensemble constitue un corps de doctrine pour la mise en œuvre de la SSI au sein des unités du CNRS.

Ces principes ont vocation à être explicités, voire complétés, dans le cadre d'instructions ou dispositions techniques dont la responsabilité d'élaboration, de diffusion et d'information relève de la chaîne fonctionnelle SSI.

La mise en œuvre des dispositions au niveau local (dans les entités) intègre le cas échéant les orientations d'autres tutelles, dans le cadre de la PSSI d'entité arrêtée par la direction de l'entité.

1) Organisation - Responsabilités

1.1 Responsabilité des différents acteurs

Les acteurs intervenant en matière de sécurité des systèmes d'information, au titre d'autorité hiérarchique ou au titre de la chaîne fonctionnelle doivent être informés de leurs responsabilités en matière de SSI.

Dans l'exercice de leur activité, ils sont liés à leur devoir de réserve voire à des obligations de secret professionnel. Ils peuvent si nécessaire faire l'objet d'une habilitation au secret de défense.

1.2 Accès aux ressources informatiques

La mise à disposition d'un utilisateur d'outils informatiques (stations de travail, postes nomades, applications…) doit être formalisée à l'arrivée, au changement de fonction et au départ de l'intéressé, qu'il soit personnel permanent ou non, CNRS ou non.

L'accès aux ressources doit être contrôlé (identification, authentification) et adapté au droit à en connaître de l'utilisateur (droits et privilèges, profil utilisateur).

Le cas échéant l'accès à des systèmes d'information ou des applications spécifiques ou encore l'exercice de fonctions de gestion de ressources informatiques peut être conditionné à une habilitation de défense.

1.3 Charte informatique

Préalablement à son accès aux outils informatiques, l'utilisateur doit prendre connaissance des droits et devoirs que lui confère la mise à disposition par son entité de ces outils.

Cette information se fait au travers d'une charte ou de dispositions équivalentes intégrées dans le règlement intérieur. Le texte correspondant doit être conforme aux prescriptions nationales (du CNRS ou de la tutelle responsable de la SSI).

1.4 Cybersurveillance

La sécurité des systèmes d'information exige de pouvoir surveiller le trafic sur le réseau et tracer les actions effectuées.

Les dispositifs mis en œuvre doivent être conformes à la réglementation en vigueur et respecter les principes de proportionnalité (adaptation du niveau des moyens à l'enjeu effectif de la sécurité) et de transparence (information des partenaires sociaux et utilisateurs).

La mise en place de tels dispositifs donne lieu à des principes et règles arrêtés préalablement et diffusés au sein du CNRS (politique de gestion des traces par exemple).

1.5 Formation, sensibilisation

La formation, la sensibilisation et l'information des différents acteurs de l'expert SSI à l'utilisateur en passant par le responsable de l'entité sont cruciales pour la sécurité. Sous la responsabilité de la chaîne fonctionnelle SSI du CNRS, des actions en ce sens sont régulièrement menées au niveau local, régional et national.

Elles font l'objet d'une planification arrêtée au niveau du comité de pilotage de la SSI et donnent lieu à un suivi dans le cadre du tableau de bord de la SSI.

1.6 Infrastructure de Gestion de Clés

Le CNRS a défini et déploie au sein des unités une Infrastructure de Gestion de Clés (IGC). Cette IGC a pour objectif de permettre, par certificats électroniques, l'authentification de personnes ou de services voire le chiffrement des données, pour les échanges et les accès à des applications sécurisées.

Le déploiement de l'IGC est à destination des personnels relevant d'unités du CNRS (qu'ils soient ou non personnels CNRS). Il peut exceptionnellement s'étendre à l'extérieur du CNRS dans le cadre de projets avec des partenaires.

L'octroi de certificats électroniques à des personnels étrangers hors Union Européenne de statut non permanent peut être soumis à autorisation.

1.7 Veille technique et juridique

Une veille technique et juridique est assurée par l'UREC en liaison avec le FSD, la DAJ pour la partie juridique et la DSI pour les applications de gestion.

1.8 Gestion de la documentation SI

La gestion de la documentation SSI est assurée par l'UREC. La documentation comprend l'ensemble des dispositions législatives et réglementaires concernant la SSI, ainsi que l'ensemble des documents d'orientation nationale (PSSI, Schéma directeur SSI) et les instructions et recommandations techniques propres au CNRS.

2) Protection des données

2.1 Disponibilité, confidentialité et intégrité des données

Le traitement et le stockage de données informatisées, l'accès à des services ou à des applications internes ou externes et de manière générale les échanges de données entre systèmes d'information doivent être réalisés selon des méthodes visant à prévenir la perte, la modification et la mauvaise utilisation des données ou la divulgation des données ayant un caractère sensible.

En particulier une sauvegarde régulière des données avec des processus de restauration validés doit être mise en place.

2.2 Protection des données sensibles

Le stockage et la transmission de données « classifiées de défense » sont interdits sauf utilisation de moyens spécifiques agréés au niveau national.

Les données non classifiées mais présentant un caractère sensible doivent identifiées et le cas échéant repérées selon un niveau de sensibilité (en s'appuyant sur la méthodologie CAPSEC par exemple).

Pour l'évaluation de la sensibilité des données, on tiendra compte du fait que l'accumulation de données a priori anodines peut conduire à une information sensible.

Il sera procédé régulièrement à un réexamen de la sensibilité des données.

Les données sensibles devront impérativement faire l'objet d'une protection au niveau du contrôle d'accès, du traitement, du stockage ou de l'échange pour en assurer la confidentialité :

- L'accès à une donnée sensible ne doit être possible qu'après authentification et contrôle de l'autorisation. Une donnée sensible ne doit pas faire l'objet d'un partage non contrôlé.
- Toute information sensible circulant sur un réseau externe doit être chiffrée.
- Tout support contenant des données sensibles transporté à l'extérieur (disquette, clé USB, cdrom, bande magnétique, etc., cela inclut aussi les ordinateurs portables) doit faire l'objet de mesure de protection contre le vol ou les informations contenues doivent être chiffrées.
- Les informations sensibles ne doivent pas être stockées ou traitées sur des systèmes informatiques non maîtrisés (cybercafé par exemple).
- Le stockage chez un prestataire externe de données sensibles est interdit, sauf dispositions contractuelles de protection ou chiffrement des données.
- Pour le stockage et l'échange informatisé de données particulièrement sensibles on devra impérativement mettre en œuvre des moyens de chiffrement, selon les dispositions définies au niveau national (cf ci-après).

2.3 Données à caractère personnel

Les traitements de données susceptibles de contenir des informations à caractère personnel (au sens de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés) doivent faire l'objet des formalités requises de déclaration ou de demande d'autorisation auprès de la CNIL, sous la responsabilité du service gestionnaire de cette procédure au CNRS.

Les CSSI des entités, sous l'autorité de leur directeur d'entité, contribuent à l'information et la sensibilisation des responsables de traitement. Ils incitent à la correction d'éventuelles anomalies et en cas de difficulté font part des éventuels incidents à leur hiérarchie et à la chaîne fonctionnelle SSI.

Les données à caractère personnel constituent des données sensibles et comme telles doivent faire l'objet de protection.

2.4 Chiffrement

Le chiffrement constitue un moyen privilégié de protection des données. Il est d'emploi obligatoire pour le stockage et l'échange de données particulièrement sensibles.

Les produits utilisés doivent faire l'objet d'un agrément au niveau national.

Tout chiffrement implique la mise en œuvre de procédures permettant de restituer en toutes circonstances les données en clair en cas de perte du secret permettant de les déchiffrer. Cela peut se faire par séquestre de clés, procédure de recouvrement, voire maintien d'une copie en clair.

Le respect de ces dispositions et la mise en œuvre effective du chiffrement sont réalisés au vu de recommandations internes et avec l'appui et le conseil de la part de la voie fonctionnelle SSI du CNRS.

2.5 Réparation, cession, mise au rebut

Avant tout envoi en réparation, cession ou mise au rebut d'un matériel, il convient de s'assurer que toutes les données ont bien été effacées par un procédé efficace et selon les recommandations techniques nationales.

Si cela s'avère impossible, à cause d'une panne par exemple, les supports concernés devront être démontés et détruits.

3) Sécurisation du Système d'information

3.1 Administration des serveurs

L'administration des serveurs est placée sous la responsabilité des administrateurs systèmes et réseaux de l'entité.

L'administration des postes serveurs par les utilisateurs eux-mêmes doit demeurer l'exception et être justifiée en termes de besoins et de compétences.

3.2 Administration des postes de travail

L'administration des postes de travail individuels est normalement placée sous la responsabilité des administrateurs systèmes et réseaux de l'entité. L'administration des postes peut être assurée par les utilisateurs eux-mêmes sous réserve de s'inscrire dans la politique de sécurité de l'unité.

3.3 Sécurisation des postes de travail et des moyens nomades

Les utilisateurs veillent à la sécurisation de leur poste de travail, des moyens nomades mis à leur disposition ou de leur portable personnel. Une vérification du niveau de sécurité doit normalement être mise en place avant l'accès au réseau.

L'accès aux postes de travail (et aux moyens nomades) doit être protégé par mots de passe. Les mots de passe constituent des données personnelles et confidentielles, ils doivent être suffisamment robustes, et ne doivent pas être divulgués ni laissés sans protection.

L'exploitation des moyens informatiques hors de leur zone de sécurité (micro-ordinateurs, portables, imprimantes déportées …) et donc plus vulnérables aux vols nécessite des mesures spécifiques adaptées (protection contre le vol, chiffrement…) de la part de l'utilisateur.

La sortie et l'utilisation à l'extérieur de l'entité de tout équipement informatique doivent avoir été autorisées.

La connexion par des moyens nomades du CNRS au système d'information d'un tiers doit respecter les règles de sécurité de ce tiers.

3.4 Contrôle d'accès

L'accès au système d'information exige une identification et une authentification préalable. L'utilisation de comptes partagés ou anonymes doit être évitée. Des mécanismes permettant de limiter les services, les données, les privilèges auxquels à accès l'utilisateur en fonction de son rôle dans l'organisation doivent être mis en œuvre dans la mesure du possible.

Les accès doivent être journalisés.

L'attribution et la modification des accès et privilèges d'un service doivent être validées par le propriétaire du service. Pour les services sensibles, un inventaire régulièrement mis à jour en sera dressé. Il importe de bien différencier les différents rôles et de n'attribuer que les privilèges nécessaires.

3.5 Sécurité des applications

La sécurité doit être prise en compte à toutes les étapes d'un projet, interne ou externe, lié au système d'information de l'entité. Pour cela, un dossier de sécurité doit accompagner chaque projet et préciser les enjeux, les méthodes, les mesures préconisées, les jalonnements et les tableaux de bord éventuels

En particulier les **applications informatiques de gestion** et les **applications internet telles que les sites Web**, doivent être sécurisées, en cohérence avec la sensibilité des informations traitées et échangées.

Les grands projets d'application de gestion doivent comporter une étude de sécurité approuvée par le RSSI de la DSI, le FSD, voire le directeur général (en tant qu'AQSSI) selon l'importance de l'application. L'analyse de sécurité correspondante peut s'inspirer utilement de la méthode EBIOS.

Les analyses de sécurité doivent intégrer les situations d'hébergement sur sites extérieurs.

3.6 Maintenance et téléaction internes

Lorsqu'elles utilisent un logiciel leur permettant d'intervenir à distance sur l'ordinateur d'un utilisateur, les personnes chargées de l'administration ou du support doivent l'en avertir et respecter les principes de la loi Informatique et Libertés.

La garantie d'une relation de confiance mutuelle repose sur le fait que l'utilisateur puisse conserver la maîtrise de son environnement.

3.7 Infogérance et télémaintenance externes

L'infogérance correspond au fait que des sociétés extérieures, chargées de gérer une partie de l'informatique du laboratoire, ont accès au SI depuis l'extérieur ou l'intérieur.

Il est alors important de mesurer les risques afin de définir précisément les droits d'accès appropriés pour ces sociétés. Les prestataires de service doivent respecter les conditions de sécurité (répondre aux mêmes normes) exposées ci-dessus pour la maintenance, auxquelles un contrôle renforcé sur les ressources mises à disposition doit être ajouté. Un contrat doit clairement préciser les responsabilités et l'imputabilité en cas d'incident.

L'externalisation de la gestion d'exploitation d'un composant critique pour le SI de l'entité est à proscrire, sauf dispositions de garantie spécifiques et validées au niveau national (UREC ou RSSI de la DSI).

Une entité utilisant la télémaintenance devra renforcer la surveillance de ces accès qui nécessitent souvent des privilèges élevés. Les contrats avec les sociétés de services devront contenir, le cas échéant, des engagements de responsabilité.

3.8 Clauses dans les marchés

Les marchés publics relatifs à des prestations informatiques (intégration de logiciels, infogérance, maintenance…) doivent comporter des clauses de confidentialité voire d'agrément et d'habilitation de personnes.

Des dispositions contractuelles types sont proposées par la chaîne fonctionnelle SSI.

L'accès au système d'information de l'unité de la part de personnels d'entreprises extérieures doit être conforme à la politique générale d'accès aux moyens informatiques. Les obligations correspondantes, notamment la signature de la charte utilisateur, doivent être mentionnées dans les dispositions contractuelles.

3.9 Réseau

Le SI doit être protégé vis-à-vis de l'extérieur à l'aide de filtres d'accès appliqués sur les équipements en tête de son réseau.

Une attention particulière doit être portée aux équipements nomades et PDA pour éviter, notamment, de servir de passerelle vis-à-vis de l'extérieur, de contaminer l'intérieur par des logiciels malveillants. D'une manière générale, leur connexion au SI ne doit pas modifier ou remettre en cause la sécurité du système d'information et doit être approuvée par le CSSI.

L'utilisation de réseaux de télécommunication externes au laboratoire met en relation des utilisateurs qui n'ont, a priori, pas les mêmes exigences de sécurité. Il est donc nécessaire de définir des modalités d'utilisation sécurisée pour les accès depuis l'extérieur comme les liaisons via ADSL. Il convient de définir les différents canaux de communication utilisés et formaliser pour chacun d'entre eux les règles d'utilisation par des contrats, des engagements de la part des utilisateurs, des tiers ou des équipes délocalisées (exemple : serveur de messagerie, sauvegardes opérées par un service externe au laboratoire).

Dans toute la mesure du possible le réseau interne doit être cloisonné afin d'isoler les différents services et usages et limiter l'impact d'incidents. En particulier il est vivement souhaitable d'isoler dans une zone semi-ouverte les services visibles de l'extérieur. De même l'accès au réseau sans fil doit être contrôlé et le réseau doit faire l'objet d'un chiffrement adapté.

Toute connexion d'un matériel au réseau doit être approuvé par le CSSI. Toute liaison vers l'extérieur autre qu'à travers le réseau de l'entité (modem, ADSL, GPRS, 3G par exemple) est interdite sauf besoins particuliers et après accord du CSSI.

3.10 Maintien du niveau de sécurité

Le maintien du niveau de sécurité (en particulier la vérification d'absence de risque lors l'installation de nouveaux matériels ou logiciels ou de connexion de matériels mobiles…) doit faire l'objet de dispositions techniques sous la responsabilité de l'UREC.

Ces dispositions doivent intégrer le maintien au cours du temps de l'état de sécurité des différents matériels : application des correctifs, mises à jour des anti-virus, pare-feu, etc.

Elles doivent préciser les conditions de surveillance du fonctionnement du SI de manière à s'assurer de son état de sécurité : analyse des journaux, vérification des vulnérabilités, suivi des avis de sécurité.

4) Mesure du niveau effectif de sécurité

4.1 Contrôle de gestion

La sécurité des systèmes d'information du CNRS fait l'objet de documents de cadrage, d'organisation et de planification.

Le contrôle de gestion de la SSI s'opère sous la responsabilité du FSD. Il donne lieu à un tableau de bord de la SSI.

4.2 Audits

Le niveau de sécurité des systèmes d'information et la conformité de mise en œuvre des recommandations sur le terrain peuvent donner lieu à des audits externes, à des missions d'inspection (au sens de visite et échanges approfondis) réalisées par le fonctionnaire de sécurité de défense et à des auto-diagnostics selon la méthodologie définie par le CNRS et mise en œuvre depuis plusieurs années.

4.3 Journalisation, tableaux de bord

Le SI doit comprendre des dispositifs ou procédures de journalisation centralisée et protégée de l'utilisation des services. L'objectif est de permettre de détecter des intrusions ou des utilisations frauduleuses, de tenter d'identifier les causes et les origines, d'éviter des contaminations d'autres sites par rebond et de remettre en place le système.

La durée de conservation (et donc de sauvegarde) des fichiers de traces à des fins de preuve est précisée dans le document relatif à la gestion des traces.

Il importe de définir, et de faire connaître aux utilisateurs, les règles d'exploitation des fichiers de traces (contenu, durée de conservation, utilisation) dans le respect du « principe de proportionnalité » et des contraintes législatives et réglementaires concernant notamment le traitement des informations à caractère personnel.

4.4 Les fichiers de traces seront systématiquement analysés afin de repérer d'éventuels problèmes et de produire des statistiques et tableaux de bord.

4.5 Posture de sécurité

En matière de sécurité des systèmes d'information, le niveau normal des recommandations faites dans le cadre de la politique interne de SSI correspond aux dispositions jaunes et oranges du plan **Vigipirate.**

Ces recommandations sont rappelées régulièrement par le FSD via les délégations régionales du CNRS.

Les dispositions internes de sécurisation doivent permettre une réactivité suffisante en cas de passage au niveau rouge de mesures propres à la SSI.

Le plan d'intervention gouvernemental PIRANET fait l'objet annuellement d'exercices destinés à tester la réactivité de la chaîne d'intervention et la faisabilité des mesures préconisées.

4.6 Mises en garde

L'utilisation de certains matériels ou logiciels peut s'avérer préjudiciable à la sécurité des systèmes d'information. Ces produits font l'objet de « mises en garde » de la part de la chaîne fonctionnelle SSI, visant soit des recommandations d'utilisation, soit une interdiction pure et simple.

4.7 Gestion d'incidents

Chaque acteur du SI, utilisateur ou administrateur doit être sensibilisé à l'importance de signaler tout incident réel ou suspecté.

Une procédure de gestion des incidents est diffusée et mise en ligne permettant aux administrateurs systèmes et réseaux, responsables SSI et directeurs d'unité de réagir à bon escient et de transmettre l'information.

Le signalement des incidents à la chaîne fonctionnelle est systématique.

L'information des autorités hiérarchiques et de la délégation régionale est impérative lorsque l'incident peut mettre en cause l'entité dans son fonctionnement, sa sécurité, sa discipline interne, son image de marque…

L'opportunité d'une information directe du FSD doit être appréciée au regard de la gravité de l'incident et/ou du caractère sensible de l'entité concernée. Cette information doit être systématique si l'incident est susceptible d'implications juridiques (dépôt de plainte par exemple).

Dans le cas d'unités mixtes, il convient d'informer et le cas échéant de se concerter avec les autres tutelles.

Les données statistiques relatives à la gestion des incidents sont intégrées dans le tableau de bord de la SSI.

Les vols d'ordinateurs ou de supports de données doivent être considérés comme des incidents de SSI et traités selon le même principe

4.8 Gestion de crise

Le plan de gestion de crise du CNRS intègre les risques liés à l'informatique ainsi que les risques susceptibles d'une incidence sur la sécurité des systèmes d'information. Pour ces incidents, le FSD est membre de la cellule de gestion de crise du CNRS.

Le FSD prévoit le dispositif organisationnel propre aux crises de nature informatique.

Il doit être informé dès le déclenchement de toute crise ayant une incidence sur la sécurité des systèmes d'information. Il veille à la bonne information des autres structures concernées dont la cellule nationale de gestion de crise du CNRS.

4.9 Plan de continuité

L'entité doit définir un plan de continuité et les procédures correspondantes. Ce plan doit permettre, dans un premier temps, de maintenir en mode dégradé les activités critiques, puis de récupérer et de restaurer toutes les fonctionnalités du système d'information.
