REGLEMENT INTERIEUR DE L'INSTITUT FRESNEL

1 - ASSEMBLEE GENERALE ET CONSEIL D'UNITE

Le Conseil de laboratoire est présidé par le directeur de l'Unité. Il a un rôle consultatif et émet un avis sur toutes les questions relatives à la politique scientifique, la gestion des ressources, l'organisation et le fonctionnement de l'Unité.

Sa composition et ses modalités de fonctionnement sont prévues en application de la décision CNRS n° 920368SOSI du 28 octobre 1992 modifiée. Le conseil de laboratoire de l'Institut Fresnel comporte des membres de droit, des membres élus et des membres nommés :

- Le(a) Directeur(trice), anisi que le(s) Directeur(trice)s Adjoint(e)(s), sont membres de droit,
- 10 membres sont élus (2 représentants du collège A et 5 représentants du collège B, 1 représentant du collège des doctorants, 2 représentants du collège ITA/IATOS),
- 8 membres sont nommés par le(a) Directeur(trice) de l'Unité, dont les membres de la direction.

La durée du mandat des membres du conseil de laboratoire est de trois ans.

Conformément à la décision CNRS n° 920368SOSI du 28 octobre 1992 modifiée, le conseil est consulté par le Directeur de l'Unité sur toute mesure relative aux moyens, à l'organisation et au fonctionnement de l'Unité.

Il se réunit au moins trois fois par an.

L'avis du conseil est recueilli par les organismes de tutelle en vue de la nomination du Directeur de l'unité.

L'assemblée générale est constituée :

- Des membres permanents du laboratoire : enseignants-chercheurs, chercheurs, ingénieurs et techniciens de l'Université d'Aix-Marseille, de l'Ecole Centrale de Marseille, du CNRS,
- Des membres non permanents : doctorants, post-doctorants, ATER
- Des personnels contractuels accueillis dans le laboratoire depuis plus d'un an.

L'assemblée générale se réunit au moins une fois par an sur convocation du Directeur. Elle peut également se réunir à la demande d'au moins ¼ des personnels permanents. Le délai minimum de convocation est de 8 jours francs.

2 - DIRECTION

La nomination de (de la) Directeur(trice) de l'Unité est prononcée conjointement par les tutelles après avis des instances compétentes du Comité national et du conseil de laboratoire, ou par défaut après avis de l'Assemblée Générale de l'Unité réduite aux permanents.

Le Directeur décide de l'utilisation de l'ensemble des moyens dont dispose l'unité. Il présente au moins annuellement un compte rendu de l'emploi des ressources. Il donne son accord à toute affectation de moyens à des membres de l'unité par des tiers. Il définit les modalités d'accueil et les conditions d'accès aux ressources applicables aux doctorants accueillis dans le laboratoire.

Les responsables d'équipes sont élus par les membres de l'équipe. Le vote doit se renouveler, au minimum, à l'issue de chaque évaluation de l'Unité.

Les représentants de thèmes sont élus par les membres du thème correspondant pour une durée minimale, renouvelable, de demi-période d'évaluation.

Le conseil scientifique interne de l'Unité est formé des membres de la direction et des représentants des thèmes (ou leur suppléant(e)).

3 - HORAIRES, CONGES, ABSENCES

La durée annuelle du travail effectif pour chaque agent de l'Unité est fonction de son établissement de tutelle et de son statut. Chaque agent doit donc se référer aux textes définis par son employeur (CNRS, Université, Ecole Centrale de Marseille).

3.1 – Horaires de travail, travail isolé

La durée hebdomadaire du travail effectif pour chaque agent de l'Unité travaillant à temps plein est définie par son employeur, conformément aux arrêtés pris par les différentes tutelles, sur cinq jours, du lundi au vendredi.

Les personnels autorisés à accomplir un service à temps partiel d'une durée inférieure ou égale à 80 % peuvent travailler selon un cycle hebdomadaire inférieur à 5 jours.

La plage horaire de travail de référence commence à 8 heures et se termine à 18 heures.

Sous réserve de l'accord du chef d'équipe, ainsi que du directeur du laboratoire, certains personnels peuvent pratiquer un horaire décalé par rapport à la plage horaire de référence.

La pause méridienne, qui n'est pas comprise dans le temps de travail, ne peut être inférieure à 45 minutes ni supérieure à 2 heures.

3.2 - Modalités d'accès aux bâtiments ZRR

Heures ouvrables pour l'accès physique aux bâtiments : de 7 heures à 20 heures 30 du lundi au vendredi.

En dehors de ces périodes, la présence d'agents doit être soumise à l'autorisation du directeur.

L'accès aux locaux du laboratoire est réservé aux personnels et personnes ayant une raison professionnelle liée au fonctionnement du laboratoire de s'y trouver.

Les activités non liées directement au fonctionnement courant du laboratoire sont proscrites et en particulier les activités commerciales (notamment de denrées alimentaires).

Par ailleurs, sous réserve d'une autorisation nominative signée par le chef d'équipe, contresignée par le directeur du laboratoire, certains personnels (au minimum 2) peuvent accéder aux locaux pendant les périodes de fermeture pour des raisons exclusivement professionnelles.

Par accès aux bâtiments ZRR on entend aussi bien l'accès physique que l'accès à distance ou virtuel.

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

L'accès de ces personnes à la ZRR est soumis à l'autorisation du Directeur d'Unité après avis favorable du Ministère de l'enseignement supérieur et de la recherche.

L'intéressé devra formaliser sa demande d'accès au moyen d'un formulaire (modèle joint en annexe), sans possibilité de mandater un tiers.

La possession d'un badge est obligatoire pour accéder à l'Unité. Ce badge est attribué aux personnels non-permanents après avis du Directeur d'Unité.

Les nouveaux entrants en attente de badge doivent signer le répertoire d'entrée et de sortie situé à l'accueil de l'Unité.

b) Pour les visiteurs

Les visites au sein d'une unité ZRR, qui se caractérisent par leur aspect temporaire et leur absence de participation directe aux activités scientifiques et techniques de l'Unité, sont soumises à l'autorisation de son Directeur. L'absence de réponse au bout d'un jour ouvrable sera considérée comme une acceptation tacite. Le Directeur doit transmettre au FSD compétent toute demande d'autorisation jugée sensible. Le FSD prendra si nécessaire l'attache des services territoriaux compétents.

Font partie des visiteurs les personnes qui viennent exercer une activité d'enseignement ou suivre un enseignement dans la ZRR, lorsque cet enseignement ne prépare pas à une thèse ou à un doctorat.

Les interventions justifiées par un risque imminent pour la vie, la sécurité des personnes et des biens ne sont pas soumises aux dispositions relatives à l'accès des visiteurs aux locaux.

Au moins un jour ouvrable avant la visite, une demande devra être adressée au Directeur d'Unité. L'autorisation accordée par le Directeur d'Unité ne pourra excéder 5 jours. Lorsque l'autorisation d'accès concerne un étudiant, elle précise que, en plus d'être limitée dans sa durée, elle est

strictement limitée dans la journée au temps de présence exigé par l'enseignement suivi (y compris les stages).

Le visiteur ne peut accéder aux locaux que muni d'un badge temporaire.

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

A leur arrivée, les visiteurs remplissent le répertoire des visites. Ils fournissent également la preuve qu'ils sont bien la personne qui a fait l'objet de l'autorisation en produisant un document officiel d'identité.

Ce répertoire doit faire l'objet d'une déclaration au Correspondant informatiques et Libertés (CIL).

Chaque visite se fait en la présence d'un ou plusieurs personnels permanents nommément désignés à cet effet chargé de contrôler, accompagner et surveiller les visiteurs.

Si nécessaire, les mesures de sécurité de l'Unité sont portées à la connaissance des visiteurs par l'accompagnateur.

En cas d'incident au cours de la visite, l'accompagnateur doit en avertir immédiatement le Directeur d'Unité.

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

3.3 Travailleur isolé

En ce qui concerne le travail isolé, deux cas sont à distinguer :

- celui où un travailleur est isolé du fait de son poste de travail (ex : atelier de mécanique)

- celui où un travailleur est présent sur son lieu de travail en dehors des horaires d'ouverture (ex : expérience en cours, contrainte de temps etc.…)

Ces cas de figure doivent être exceptionnels et donner lieu à une **autorisation expresse du Directeur.** Ce dernier prendra toutes les mesures nécessaires pour assurer leur sécurité. Et notamment, le port **obligatoire** d'un DATI (dispositif d'alarme pour travailleur isolé) s'impose.

Dans tous les cas, les personnels doivent respecter les consignes d'hygiène et de sécurité affichées dans les locaux mis à leur disposition.

3.4 Congés annuels

Le nombre de jours de congés dépend de l'établissement de tutelle, du statut et de la durée hebdomadaire du travail de l'agent. Pour les personnels dont les congés doivent être gérés par le laboratoire, le nombre annuel de congés prend en compte les jours de RTT (Réduction du Temps de Travail) compte tenu de la durée hebdomadaire du travail adoptée dans l'Unité.

Les jours RTT sont utilisés dans les mêmes conditions que les jours de congés annuels.

Les personnels peuvent bénéficier de jours de congés supplémentaires, appelés "jours de fractionnement" dans les cas suivants : 1 jour si l'agent prend 5, 6 ou 7 jours en dehors de la période du 1er mai au 31 octobre et de 2 jours si ce nombre est au moins égal à 8 jours.

Les jours de congés sont accordés par le Directeur d'unité, après avis du responsable hiérarchique, sous réserve des nécessités de service.

Le report des jours de congés annuels ainsi que les jours RTT non utilisés, sont autorisé jusqu'au 28 février de l'année n+1 pour les personnels CNRS, et jusqu'au 31 décembre de l'année n+1 pour les personnels universitaires. Les jours qui n'auront pas été utilisés à cette date seront définitivement perdus, sauf si ces jours ont été déclarés dans un Compte Epargne Temps.

Les périodes de fermeture (été et Noël) seront définies et communiquées aux personnels en début d'année civile.

Le nombre de jours ouvrables de congés obligatoires sera par conséquent à déduire du nombre de congés annuels des agents, selon leur tutelle d'appartenance.

- Pour les agents CNRS

Horaire hebdomadaire	Congés annuels	Durée annuelle de travail	Observations
38 h 30	44 j (dont 12 RTT)	1607 h	<u>Jours de fractionnement :</u> -1 jour si le nombre de jours de congés pris en dehors de la période du 1er mai au 31 octobre est de 5, 6 ou 7 jours, - 2 jours si le nombre de jours de congés pris en dehors de la période du 1er mai au 31 octobre est au moins égal à 8 jours. **Maximum : 46 jours de congés**

Congés à prendre entre le 1er janvier et le 31 décembre de l'année N.

- Pour les agents ECM

Horaire hebdomadaire	Congés annuels	Durée annuelle de travail	Observations
38H51	53 j (dont 23 RTT)	1607 h	<u>Jours de fractionnement :</u> -1 jour si le nombre de jours de congés pris en dehors de la période du 1er mai au 31 octobre est de 5, 6 ou 7 jours, - 2 jours si le nombre de jours de congés pris en dehors de la période du 1er mai au 31 octobre est au moins égal à 8 jours. **Maximum : 55 jours de congés**

Congés à prendre entre le 1er septembre de l'année N et le 31 août de l'année N+1

- Pour les agents AMU

Horaire hebdomadaire	Congés annuels	Durée annuelle de travail	Observations
37h30	47 j (dont 22 RTT)	1607h	Jours de fractionnement : - 1 jour si le nombre de jours de congés pris en dehors de la période du 1er mai au 31 octobre est de 5, 6 ou 7 jours, - 2 jours si le nombre de jours de congés pris en dehors de la période du 1er mai au 31 octobre est au moins égal à 8 jours. **Maximum : 58 jours de congés**
39h10	56 j (dont 31 RTT)		

Congés à prendre entre le 1er septembre de l'année N et le 31 août de l'année N+1.

3.4.1 Compte-épargne temps

Le Décret n° 2009-1065 du 28 août 2009 et son arrêté d'application du 28 août 2009 modifie le décret n° 2002-634 du 29 avril 2002 et le décret n° 2008-1136 du 03 novembre 2008 relatifs au CET dans la fonction publique.

Les jours de congés annuels ainsi que les jours de RTT non utilisés au 31 décembre peuvent être versés sur un Compte Epargne Temps (CET) dans les conditions statutaires prévues.

Bénéficiaires :

Sont bénéficiaires les agents dont les Etablissements ont mis ce dispositif en place. Un Compte Epargne Temps peut être ouvert, à leur demande, par les agents titulaires et non titulaires ou accueillis en détachement s'ils sont employés de manière continue depuis au moins un an dans une administration de l'Etat ou d'un établissement public en relevant.

3.4.2 Durée des absences de service pour congés

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

Suivi des congés :

Afin de pouvoir adapter l'organisation du travail, les personnels dont les congés doivent être gérés par le laboratoire doivent effectuer leurs demandes de congés auprès du directeur d'unité, après accord de leur responsable d'équipe. Pour les personnels de l'Université d'Aix Marseille, de l'Ecole Centrale de Marseille et du CNRS, le délai de prévenance est de 8 jours.

Le suivi des congés (annuels et RTT) est réalisé dans l'Unité sous la responsabilité du directeur (notamment pour la mise en œuvre du CET).

3.5 Absences

3.5.1 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 indiquant la durée prévisible de l'indisponibilité.

Tout accident corporel survenant dans le cadre de l'activité professionnelle sera immédiatement déclaré auprès du directeur de l'Unité.

3.5.2 Missions

Tout agent se déplaçant pour l'exercice de ses fonctions doit être en possession d'un ordre de mission établi une semaine avant le déroulement de la mission pour les déplacements en France, un mois avant le déroulement de la mission pour les déplacements à l'étranger. Ce document est obligatoire du point de vue administratif et juridique ; il assure la couverture de l'agent au regard de la réglementation sur les accidents de service.

L'agent amené à se rendre directement de son domicile sur un lieu de travail occasionnel sans passer par sa résidence administrative habituelle, est couvert en cas d'accident du travail sous réserve de disposer d'un ordre de mission (sauf si le lieu occasionnel de mission est situé dans la même localité que la résidence administrative).

4 - FORMATION

Le plan de formation de l'Unité est soumis pour avis au Conseil de Laboratoire.

Les responsables d'équipe de l'Unité informent et conseillent les personnels de leur équipe pour leurs besoins et demandes de formation. Ils participent, auprès du directeur de l'unité et du correspondant formation, à l'élaboration et au bilan du plan de formation de l'Unité.

5 - DIFFUSION DES RESULTATS SCIENTIFIQUES

5.1 Confidentialité

Chacun est tenu de respecter la confidentialité des travaux qui lui sont confiés lors de collaborations ou de contrats. Chacun est également tenu de respecter la confidentialité des travaux de ses collègues.

5.2 Publications

Les chercheurs sont incités, avant publication ou communication de leurs travaux, à identifier une valorisation potentielle (dépôt de brevet par exemple) de leur travail qui pourrait conduire à une procédure de protection. Les chercheurs informeront le directeur de l'unité avant d'initier une procédure de valorisation.

Concernant les questions de confidentialité et de publication, dans le cas de travaux effectués en partenariat avec des tiers, il est obligatoire de respecter les termes de la convention (contrat industriel, subvention, contrat Européen…).

Les publications font apparaître l'appartenance à l'Unité et le rattachement aux tutelles sous la forme décrite dans le contrat quinquennal établi avec les établissements de tutelle.

5.3 Cahier de laboratoire

Tous les personnels de recherche de l'unité sont fortement incités à tenir un cahier de laboratoire afin de garantir le suivi, la protection et la traçabilité des résultats de leurs travaux. Pour les travaux réalisés dans le cadre d'un contrat à justifier (coût complet) ce cahier de laboratoire ainsi qu'un cahier d'utilisation des équipements associés sont obligatoires.

Les cahiers de laboratoire appartiennent aux tutelles de l'unité et sont conservés au laboratoire même après le départ d'un personnel. Ils peuvent être requis en cas d'audit interne ou externe.

Les cahiers de laboratoire sont disponibles auprès du service Partenariat et Valorisation de la délégation régionale du CNRS.

6 – HYGIENE ET SECURITE

S'il incombe au directeur de veiller à la sécurité et à la protection des personnels et d'assurer la sauvegarde des biens de l'Unité, chacun doit se préoccuper de sa propre sécurité et de celle des autres. Les membres du laboratoire devront observer les consignes de sécurité rappelées dans l'ANNEXE 1 et affichées sur le panneau d'affichage situé dans le couloir des services administratifs et sur l'intranet de l'Institut Fresnel.

L'assistant de prévention (agent chargé de la mise en œuvre des règles d'hygiène et de sécurité) assiste et conseille le directeur, il informe et sensibilise les personnels travaillant dans l'Unité pour la mise en œuvre des consignes d'hygiène et sécurité.

Composition du CLHSCT :

Représentant de l'administration avec voix consultative :

- Le Directeur de l'Institut Fresnel, Président du CLHSCT

Membre de droit avec voix consultative

- L'assistant de prévention de l'Institut Fresnel, secrétaire administratif du CLHSCT
- Représentants du personnel avec droit de vote - 2 représentants de l'administration
- 1 représentant des chercheurs
- 1 représentant du personnel technique
- 1 représentant du service technique de l'Institut Fresnel

Invités permanents avec voix consultative

- Le conseiller de prévention du CNRS
- Le conseiller de prévention d'AMU
- Le médecin de prévention du CNRS
- Le médecin de prévention d'AMU

Experts invités avec voix consultative

- Le référent pour les risques chimique et biologique
- Le référent pour le risque électrique
- Le référent pour le risque laser
- Le référent pour le risque lié au vide,
- Le référent pour le risque lié aux machines-outils.

L'identité de l'assistant de prévention, la composition nominale du comité local d'hygiène, de sécurité et des conditions de travail ainsi que les coordonnées de tous ses membres sont disponibles sur l'intranet du site web. Ces renseignements sont affichés sur le panneau d'affichage dédié.

Les dispositions à prendre en cas d'accident et d'incendie font l'objet d'un document spécifique et sont affichées sur le même panneau d'affichage.

Le registre de santé et de sécurité au travail dans lequel les personnels a la possibilité de consigner tous les incidents, les accidents, leurs les observations et les suggestions relatives à la prévention des risques et à l'amélioration des conditions de travail est placé à la disposition du personnel dans la loge à l'entrée principale du bâtiment.

L'assistant de prévention et/ou le référent de chaque catégorie, doit sensibiliser les personnels, dès leur arrivée, et leur fournir les informations nécessaires à l'accomplissement de leur travail et au respect des consignes générales de sécurité.

Il est interdit aux personnels de fumer sur les lieux de travail.

Dans les locaux de l'Institut Fresnel, les risques spécifiques suivants ont été identifiés :

- Electricité
- Chimie, Biologie
- Vide
- Lasers
- Machines tournantes

Tous les locaux présentant un risque particulier relevant d'une ou plusieurs catégories précédentes font l'objet d'une signalétique particulière.

Pour toutes les catégories précédentes, des consignes de sécurité minimales jointes dans l'ANNEXE 1 devront être respectées.

Concernant la mécanique, la seule personne habilitée à utiliser les machines tournantes est le responsable de l'atelier. Une seule dérogation a été accordée à un autre membre de l'Institut (équipe RCMO). L'utilisation des machines est assujettie à l'observation scrupuleuse des consignes de sécurité.

En cas de danger grave **et** imminent, le personnel du laboratoire a le droit d'exercer son droit de retrait. Le danger grave est un danger susceptible de produire un accident ou une maladie entraînant la mort ou paraissant devoir entraîner une incapacité permanente ou temporaire prolongée. Le danger doit également être imminent, c'est-à-dire susceptible de survenir dans un délai très bref.

L'agent doit immédiatement aviser le directeur de l'unité et son employeur de l'existence d'un danger grave et imminent et peut également en informer un membre du CHSCT. L'administration doit alors procéder à une enquête à laquelle il est recommandé d'associer un membre du CHSCT. L'administration doit prendre les mesures permettant de remédier à la situation.

Un registre de signalement d'un danger grave et imminent est placé auprès du doyen de la faculté des sciences et techniques de Saint-Jérôme pour le personnel d'AMU et auprès du Délégué Régional pour le personnel CNRS.

7 – UTILISATION DES MOYENS INFORMATIQUES

L'utilisation des moyens informatiques est soumise à des règles explicitées dans la charte informatique. Cette charte est avant tout un code de bonne conduite. Elle a pour objet de préciser la responsabilité des utilisateurs, en accord avec la législation, et doit être signée par tout nouvel arrivant.

Des traitements automatisés de données à caractère personnel ayant pour objet la gestion des traces générées par l'utilisation des moyens télématiques et informatiques sont créés au Centre National de la Recherche Scientifique – cf. Décision n°04P014DSI du 11 octobre 2004 portant création de traitements informatisés ayant pour objet la gestion des traces générées par l'utilisation des moyens informatiques et des services réseau au CNRS.

Les données à caractère personnel sont conservées un an.

Le droit d'accès prévu par l'article 38 et suivants de la loi n°78-17 du 6 janvier 1978 modifiée s'exerce auprès du responsable du traitement au sein de l'unité concernée.

Cette charte informatique est annexée au présent règlement intérieur.

8 – ACCUEIL DES PERSONNELS ET NOUVEAUX ARRIVANTS

Dans un souci d'information et de protection, le directeur d'unité devra porter à la connaissance des agents titulaires et non permanents, dès leur arrivée dans l'unité, le contenu des documents suivants :

- Le règlement intérieur,

- La charte informatique

Et ceux-ci devront attester en avoir pris connaissance.

9 - DATE D'EFFET

Règlement applicable au **01.02.2020**

Date d'approbation du présent règlement intérieur par le conseil de laboratoire : **08.01.2020**

Signature du directeur d'Unité :

Signature du(de la) Délégué(e) Régional(e) du CNRS :

ANNEXES

ANNEXE 1 - HYGIENE ET SECURITE

Des risques spécifiques à l'unité ont été répertoriés. Ils sont au nombre de 5 :

- les risques en électricité,
- les risques liés aux lasers,
- les risques en chimie/biologie,
- les risques liés au vide,
- les risques liés aux machines tournantes.

Chaque risque fait l'objet d'une règlementation spécifique.

- **RISQUES ELECTRIQUES**

Pour ce qui concerne les risques électriques, les consignes suivantes devront être respectées :

- Eviter le surnombre de multiprises, les rallonges à enrouleur.
- Faire une demande de travaux ou de modification de l'installation.
- Eviter de brancher des convecteurs de chauffage électriques, cafetières, bouilloires, plaques de cuisson.
- Retirer les prises des alimentations stabilisées la nuit (calculatrices, pc portables…).
- En cas de coupure de courant, ne pas remonter le disjoncteur. Prévenir le référent pour les risques électriques, pour la recherche de l'origine du problème et le rétablissement du courant.

- **RISQUES LIES AUX LASERS**

L'utilisation d'un laser comporte des risques pour l'œil et la peau, ainsi que des risques d'incendie, d'électrocution, ...

La prévention de ces risques passe par la formation et l'information du personnel étant amené à manipuler des lasers ou à rentrer dans des salles où des lasers sont en fonctionnement (chercheur, personnel technique, doctorant, stagiaire,).

Prévention des risques

Des formations sur la sécurité laser (connaissance des risques, moyens de prévention, choix de lunettes, consignes de sécurité,) sont distribuées à l'arrivée des personnels dans l'unité par le référent pour les questions de sécurité laser.

Un document PDF sur la sécurité laser (correspondant à la formation dispensée aux personnels du laboratoire) est disponible sur le site Intranet du laboratoire.

Les normes relatives aux sécurités des appareils à lasers et les protections individuelles (permettant de choisir les lunettes adaptées) sont consultables auprès du référent pour les questions de sécurité laser.

Outre les informations données dans ces documents et la formation dispensée, les dispositions suivantes devront être suivies lors de l'utilisation de lasers au laboratoire :

Signalétique

Les appareillages utilisant des lasers de classe 3B ou 4 feront l'objet d'une signalétique placée sur les portes d'entrée des salles concernées (sigle international de danger laser). Un voyant lumineux indiquant le fonctionnement du laser sera placé à l'extérieur de ces salles.

Moyens de protection

Pour protéger les yeux, des lunettes seront mises à disposition des personnes travaillant sur ces appareillages. Le port des lunettes de protection est obligatoire dans les salles où sont utilisés des lasers de classe 3B ou 4. Les lunettes seront de préférence stockées à l'entrée de la salle.

Arrivée d'un nouveau laser au laboratoire

Tout nouveau laser arrivant au laboratoire doit être signalé au référent pour les questions de sécurité laser. Des lunettes de protection appropriées doivent être mises à disposition des personnes travaillant avec les lasers.

Remarques : les DEL et diodes lasers sont soumises aux mêmes réglementations que les lasers.

- **RISQUES RELATIFS A LA CHIMIE ET A LA BIOLOGIE**

Un document PDF sur les risques liés à la manipulation de produits biologiques ou chimiques (correspondant à la formation dispensée aux personnels du laboratoire) est disponible sur le site Intranet du laboratoire.

Les normes relatives à la manipulation de produits biologiques ou chimiques sont consultables auprès du référent correspondant.

Prévention des risques

Certains produits chimiques ou biologiques sont corrosifs (acides, bases), toxiques, nocifs, inflammables, CMR (cancérigènes, mutagènes, reprotoxiques) peuvent nuire à l'environnement... Ils demandent donc un usage, un stockage, un étiquetage et une élimination adaptés.

Moyens de protection

Pour se protéger des risques chimiques associés à certains produits, porter blouse, lunettes et gants et manipuler les produits dans une sorbonne à l'aide de pipettes. Certains produits particuliers (acide fluorhydrique) exigent des précautions particulières à respecter.

Stockage

Les produits doivent être stockés dans des enceintes aérées à l'abri de sources de chaleur. Ils doivent être séparés selon leur nature (acides/produits inflammables par exemple)

Les déchets

Des bidons sont prévus pour chacun type de déchets (acides, bases, solvants organiques halogénés ou non halogénés...). Certaines matières toxiques exigent des traitements particuliers.

Etiquetage

Chaque produit doit être correctement étiqueté dans un récipient adapté portant une étiquette qui indique le contenu et le risque associé (corrosif, toxique, inflammable,...).

- **RISQUES LIES AUX SYSTEMES SOUS VIDE**

Un document PDF sur les risques liés à la manipulation de systèmes sous vide (correspondant à la formation dispensée aux personnels du laboratoire) est disponible sur le site Intranet du laboratoire.

Les enceintes d'évaporation sous vide, qu'elles soient en fonctionnement ou même à l'arrêt, présentent des risques importants au niveau humain, matériel et environnemental.

Lorsque les installations ne sont pas utilisées correctement (ex. : gaz ou matériaux inappropriés ou interdits), il y a risque de panne partielle ou totale du matériel. Dans ce cas il peut y avoir un risque important de pollution de l'environnement.

Les normes relatives à la manipulation des systèmes sous vide sont consultables auprès du référent correspondant.

Prévention des risques

Pour le personnel qui utilise ou non ces systèmes et qui entrent dans les salles concernées, il y a :

- Risque mortel d'électrocution (HT 10kV),

- Risque de blessure mortelle en cas de dysfonctionnement des sécurités machines (sécurités instrumentées, i.e. transmetteurs de pression, vannes d'échappement…) et des sécurités physiques (grillages de protection…).

Des formations sur l'utilisation des systèmes sous vide (connaissance des risques, moyens de prévention, mise en place de protections physiques, consignes de sécurité...) sont distribuées à l'arrivée des personnels dans l'unité par le référent pour les risques relatifs au vide.

Le personnel qui travaille sur les systèmes sous vide doit donc, avant chaque utilisation, veiller, en relation avec le référent à ce que la maintenance préventive des sécurités machines ait bien été effectuée. Il doit donc s'informer auprès du référent des risques relatifs au vide et respecter les dispositions nécessaires au maintien de la sécurité.

Aucune intervention électrique sur ces systèmes ne doit être effectuée par une personne autre que les référents des risques relatifs au vide et à l'électricité.

- **RISQUES LIES AUX MACHINES TOURNANTES**

L'atelier de mécanique est un lieu à risques où se trouvent des machines tournantes, coupantes et pliantes.
Les risques associés sont souvent importants et sont les suivants : risque d'entrainement, choc, écrasement, cisaillement, sectionnement, coupure, projection et brûlure.

Il est strictement interdit d'utiliser ces machines. Les seules personnes autorisées sont le responsable de l'atelier et une personne habilitée par la direction.

ANNEXE 2 – CHARTE INFORMATIQUE

Charte pour l'usage
de ressources informatiques et de services Internet

Décision n°070007DAJ du 18 janvier 2007 portant approbation des modifications de la charte pour l'usage de ressources informatiques et de service Internet

Ce texte, associé au règlement intérieur des entités, a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation, afin d'instaurer un usage conforme des ressources informatiques et des services Internet relevant du CNRS et le cas échéant d'autres établissements. Ces ressources et services constituent un élément important du patrimoine scientifique et technique du CNRS.

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

1. Définitions

On désignera de façon générale sous le terme « *ressources informatiques* » : les réseaux, les moyens informatiques de calcul ou de gestion locaux, ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau de l'entité, les logiciels, les applications, les bases de données…

On désignera par « *services Internet* » : la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses : web, messagerie, forum, téléphonie IP (Internet Protocol), visioconférence…

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

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

2. Accès aux ressources informatiques et services Internet

L'utilisation des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder sont destinés à l'activité professionnelle des utilisateurs conformément à la législation en vigueur. L'activité professionnelle doit être entendue comme celle définie par les textes spécifiant les missions du CNRS.

L'utilisation des ressources informatiques partagées de l'entité et la connexion d'un équipement privé et extérieur (tels qu'un ordinateur, commutateur, modem, borne d'accès sans fil…) sur le réseau sont soumises à autorisation du responsable de l'entité et aux règles de sécurité de l'entité. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation de l'activité professionnelle qui l'a

justifiée.

L'entité peut en outre prévoir des restrictions d'accès spécifiques à son organisation (certificats électroniques, cartes à puce d'accès ou d'authentification, filtrage d'accès sécurisé,).

3. Règles d'utilisation et de sécurité

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

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 :

3.1 Règles de sécurité

- il doit appliquer les recommandations de sécurité de l'entité à laquelle il appartient et notamment se conformer aux dispositifs mis en place par l'entité pour lutter contre les virus et les attaques par programmes informatiques,

- il lui appartient de protéger ses données en utilisant différents moyens de sauvegarde, individuels ou mis à sa disposition,

- il doit assurer la protection de ses informations et plus particulièrement celles considérées comme sensibles au sens de la politique de sécurité des systèmes d'informations (PSSI du CNRS). En particulier, il ne doit pas transporter sans protection (telle qu'un chiffrement) des données sensibles sur des supports non fiabilisés tels que ordinateurs portables, clés USB, disques externes, etc.… Ces supports qualifiés d'« informatique nomade » introduisent une vulnérabilité des ressources informatiques et comme tels doivent être soumis aux règles de sécurité de l'entité et à une utilisation conforme aux dispositions de la présente charte,

- il doit garantir l'accès à tout moment à ses données professionnelles dans le cadre de la politique de recouvrement [1] de données mise en œuvre au sein de l'entité,

- il ne doit pas quitter son poste de travail ni ceux en libre-service en laissant des ressources ou services accessibles.

3.2 Règles d'utilisation

- Toute information est professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'utilisateur de procéder au stockage éventuel de ses données à caractère privé dans des répertoires explicitement prévus à cet effet et intitulés « privé ». La protection et la sauvegarde régulière des données de ces dossiers incombent à l'utilisateur, la responsabilité de l'entité ne pouvant être engagée quant à la conservation de cet espace,

- il doit suivre les règles en vigueur au sein de l'entité pour toute installation de logiciel et ne pas télécharger ou utiliser de logiciels ou progiciels sur le matériel de l'entité sans autorisation explicite. Notamment, il ne doit pas installer de logiciels à caractère ludique, ni contourner les restrictions d'utilisation d'un logiciel. Les logiciels doivent être utilisés dans les conditions des licences souscrites,

- il doit veiller à la protection des différents moyens d'authentification personnels. En particulier, il doit choisir des mots de passe sûrs, gardés secrets et en aucun cas il ne doit les communiquer à des tiers. Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de communiquer son mot de passe, il devra veiller dès que possible au changement de ce dernier. Il doit également protéger son certificat électronique par un mot de passe sûr gardé secret. Comme la signature manuscrite, le certificat électronique est strictement personnel et l'utilisateur s'engage à n'autoriser personne à en faire usage à sa place,

- il doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater,

- il s'engage à ne pas mettre à la disposition d'utilisateur(s) non autorisé(s) un accès aux ressources informatiques ou aux services internet, à travers des matériels dont il a l'usage,

[1] Le recouvrement est le dispositif de secours permettant à une personne habilitée d'accéder à des données lorsque le mécanisme principal n'est plus utilisable (perte ou destruction de clé, oubli de mot de passe...) ou en cas d'empêchement de l'agent détenteur.

- il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou masquer son identité,

- il ne doit pas accéder aux informations et documents conservés sur les ressources informatiques autres que ceux qui lui sont propres, et ceux qui sont publics ou partagés. Il ne doit pas tenter de les lire, modifier, copier ou détruire, même si l'accès est techniquement possible.

4. Respect de la loi informatique et libertés[2]

Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers soumis aux dispositions de la loi informatique et libertés, il doit accomplir les formalités requises par la CNIL par l'intermédiaire de la direction des systèmes d'information du CNRS en concertation avec le directeur de son entité et veiller à un traitement des données conforme aux dispositions légales. Il est rappelé que cette procédure n'est valable que pour le traitement défini dans la demande et pas pour le fichier lui-même.

5. Respect de la propriété intellectuelle

L'utilisateur ne doit pas reproduire, télécharger, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

6. Préservation de l'intégrité des ressources informatiques

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou 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, téléphonie IP…)

7.1 Internet

Internet est un outil de travail ouvert à des usages professionnels dont l'utilisation doit respecter des principes généraux et des règles propres aux divers sites qui les proposent, ainsi que dans le respect de la législation en vigueur.

En particulier, l'utilisateur :

- 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 habilités,

- ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède,

- ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers,

[2] Le Guide CNIL du CNRS, édité en 2006, reprend les principes clés pour la création ou l'utilisation des traitements de données à caractère personnel (les droits et obligations de chacun et les formalités à engager).

- ne doit pas utiliser ces services pour proposer ou rendre accessibles aux tiers des données et informations confidentielles ou contraires à la législation en vigueur,

- ne doit pas déposer des données sur un serveur interne ou ouvert au grand public (google, free, orange, …) ou sur le poste de travail d'un autre utilisateur sans y être autorisé par les responsables habilités,

- doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions…,

- n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice au CNRS,

- doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire.

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

7.2 Messagerie électronique

La messagerie électronique est un outil de travail ouvert à des usages professionnels.

- Tout message sera réputé professionnel sauf s'il comporte une mention particulière et explicitée dans son objet indiquant son caractère privé ou s'il est stocké dans un espace privé de données.

▪ Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

▪ La transmission de données classifiées[3] est interdite sauf dispositif spécifique agréé et la transmission de données dites sensibles doit être évitée ou effectuée sous forme chiffrée.

▪ L'utilisateur doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages de masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

► L'évolution permanente des technologies de l'informatique met à disposition des utilisateurs de nouveaux services qui peuvent être accessibles depuis le réseau de leur entité. Ces nouvelles technologies, qui peuvent présenter un risque de vulnérabilité particulier, ne peuvent être utilisées qu'après accord préalable du responsable de l'entité et dans le strict respect de la politique de sécurité des systèmes d'informations (PSSI du CNRS).

8. Analyse et contrôle de l'utilisation des ressources

Pour des nécessités de maintenance et de gestion technique, de contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus, l'utilisation des ressources informatiques et des services internet, ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de le législation applicable et notamment de la loi sur l'informatique et des libertés.

L'utilisateur dont le poste fait l'objet d'une maintenance à distance doit être préalablement informé.

[3] Il s'agit des données classifiées de défense qui couvre le « confidentiel défense », le « secret défense » et le « très secret défense ».

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

9. Traçabilité

Le CNRS est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des donnés échangées.

Par conséquent des outils de traçabilité sont mis en place sur tous les systèmes d'information.

Le CNRS a procédé auprès de la CNIL à une déclaration qui mentionne notamment la durée de conservation des traces et durée de connexion, en application de la loi en vigueur.

10. Rappel des principales dispositions légales

Il est rappelé que l'ensemble des agents CNRS quel que soit leur statut sont soumis à la législation française en vigueur et notamment :

► la loi du 29 juillet 1881 modifiée sur la liberté de la presse,

► la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés,

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

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

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

► les dispositions du code de propriété intellectuelle relative à la propriété littéraire et artistique.

11. Application

La présente charte s'applique à l'ensemble des agents des entités du CNRS quel que soit leur statut, et plus généralement à l'ensemble des personnes, permanents ou temporaires qui utilisent, à quelque titre que ce soit, les ressources informatiques et services internet de l'entité, ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir du réseau de l'entité.

La charte doit être portée à la connaissance des personnes visées à l'alinéa précèdent par tous moyens et notamment :

- par envoi sur messagerie lorsqu'un compte est ouvert pour un utilisateur, celui-ci devant déclarer avoir pris connaissance de la présente charte,

- par voie d'affichage dans les locaux de l'entité,

- par voie d'annexe au règlement intérieur de l'entité,

- ou par remise d'un exemplaire papier de la charte.

La charte peut être annexée aux contrats de travail et aux conventions de marché public dont l'exécution implique l'accès aux ressources informatiques et services internet du CNRS.

La présente charte est disponible en anglais. Seule la version française fait foi.

ANNEXE 2bis – CHARTE INFORMATIQUE

English Version

Charter for the use of

IT resources and Internet services

The purpose of this document, in conjunction with the entities' by-laws, is to set forth the responsibility of users in-line with legislation, so as to establish compliant use of the IT resources and Internet services which the CNRS and, where applicable, other establishments, manage. These resources and services represent a major element of the CNRS' scientific and technical asset base.

The due and proper operation of the information system requires compliance with the relevant legislative and regulatory provisions and, in particular, security, processing performance levels and the retention of professional data.

1. Definitions

Generally speaking, the following shall be designated as "*IT resources*": the networks, the IT calculation or local management equipment, and that which is able to be remotely accessed, either directly or in cascade mode from the entity's network, the software, applications, databases…

The following shall be designated as "*Internet services*": the provision by local or remote servers of sundry exchange and information resources: web, message application, chat-room, IP (Internet Protocol) telephony, videoconferencing…

"*User*" shall mean the person having access to, or using, the IT resources and Internet services no matter what his/her status may be.

"*Entity*" shall mean all the entities created by the CNRS in order to carry out its assignments such as, in particular, its in-house or combined research units and the administrative departments and divisions.

2. Access to IT resources and Internet services

Use of the IT resources and Internet services, and the network to access the former, is destined for the professional activity of users in compliance with effective legalisation. Professional activity shall be understood as having the meaning defined in the documents setting forth the CNRS' assignments.

Use of the entity's shared IT resources and the connection of private, external equipment (such as a computer, switch, modem, wireless access station…) to the network is subject to the authorisation of the entity's manager and to the entity's security rules. Such authorisations shall be strictly personal and may not, under any circumstances, be transferred to a third party, even temporarily. They may be withdrawn at any time. All authorisations shall be cancelled when the professional activity justifying such comes to an end.

In addition, the entity may introduce access restrictions which are specific to its organisation (electronic certificates, access or authentication chip cards, secure access filtering,…).

3. Rules of use and security

All users are responsible for the use made of the IT resources to which they have access.

Use of these resources must be rational and compliant in order to avoid saturation or their misuse for personal purposes.

In particular:

3.1 Security rules

■ they shall apply the security recommendations made by the entity to which they belong and, in particular, comply with the systems implemented by the entity to combat viruses and attacks by IT programs,

■ they are responsible for protecting their data by using various individual back-up methods, or those provided to them,

■ they shall protect their information and, particularly, that which is deemed as being sensitive within the meaning of the information systems' security policy (CNRS ISSP (PSSI)). Notably, they shall not transport, without relevant protection (such as encryption), sensitive data on mediums which have not been burnt-in, such as laptops, USB keys, external hard drives, etc… These mediums, which are known as "mobile IT equipment", make the IT resources vulnerable and shall therefore be subject to the entity's security rules and shall be used in accordance with the provisions of this charter,

■ they shall guarantee permanent access to their professional data within the context of the data recovery policy[1] implemented within the entity,

■ they shall not leave their work station, or the work stations which are available for use by everyone, without first shutting-down the resources or ensuring that the services are not accessible.

3.2 Rules of use

■ All information is considered as being professional with the exception of data which the

user specifically identifies as relating to his/her private life. Consequently, the user is responsible for storing any personal data in directories which are specifically created for this purpose and which are designated as being "private".

The user is responsible for the protection and regular back-up of the data in these files and the entity may not be held liable as regards the retention of this storage space,

■ Users shall comply with the effective rules within the entity as regards installing any and all software and shall not download onto, or use software or software packages on, the entity's equipment without express authorisation.

In particular, they shall not install game-type software, or fail to comply with the restrictions relating to use of a software application. The software shall be used under the conditions of the licences granted,

■ they shall ensure the protection of the various personnel means of authentication. In particular, they shall choose fail-safe passwords, which shall be kept secret, and which they shall under no circumstances pass-on to third parties. If, in exceptional and one-off circumstances, a user were to be obliged to communicate his/her password, he/she shall ensure that the latter is changed as soon as reasonably possible. He/she shall also protect his/her electronic certificate by a fail-safe password which he/she shall keep secret. As with handwritten signatures, the electronic certificate is strictly personal and the user undertakes not to allow anyone to use it in his/her place,

■ they shall report any attempted hacking of their account and, generally, any and all anomaly which they may note,

■ they undertake not to provide (an) unauthorised user(s) with access to the IT resources or to the Internet services, via the equipment which they are entitled to use,

[1] Recovery is the safety measure allowing an authorised person access to data when the main system is no longer able to be used (loss or destruction of the key, forgotten password,...) or in the event of the unavailability of the key owner.

■ they shall not use, or attempt to use, accounts other than their own or conceal their identity,

■ they shall not access information and documents saved in the IT resources other than those belonging to them, and those which are either public or shared. They shall not attempt to read, modify, copy or destroy them, even if access thereto is technically possible.

4. Compliance with the Act on information technology and civil liberties[2]

If, whilst carrying out his/her work, the user is obliged to create files which are subject to the provisions of the Act "*informatique et libertés",* he/she shall carry out the formalities required by the CNIL through the CNRS' information systems' division, together with the manager of his/her entity and shall ensure that the data is processed in accordance with legal provisions. It is hereby stipulated that this procedure is only valid for the processing defined in the request and not for the file itself.

5. Respect for intellectual property

The user shall not reproduce, download, copy, distribute, modify or use software, databases, web pages, photographs or other creations which are protected by copyright or by a proprietary claim, without having obtained the prior authorisation of the holder of such

rights.

6. Preservation of the integrity of the IT resources

The user undertakes not to voluntarily cause disruption to the due and proper operation of the IT resources and networks, either by abnormal manipulation of the equipment, or by installing parasite software known under the generic name of viruses, Trojan horses, logic bombs...

All research or other work which may cause a violation of the rule set forth in the previous paragraph may only be carried out with the authorisation of the entity's manager, and in strict compliance with the rules which may be defined in this case.

7. Use of Internet services (web, message application, chat-room, IP telephony…)

7.1 Internet

The Internet is a work tool which is available for professional use and its use shall comply with the general principles and the rules which are specific to the different sites which offer such professional content, and with effective legislation.

In particular, the user:

■ shall not log-on, or attempt to log-on, to a server by means other those complying with the provisions provided for by such server, or without being authorised to do so by the authorised managers,

■ shall not carry out acts which intentionally compromise the security or due and proper operation of the servers to which he/she has access,

■ shall not take the identity of any and all other person and shall not intercept communications between third parties,

■ shall not use these services to offer, or to provide, third parties with data and information which is confidential or which violates effective legislation,

[2] The CNRS' CNIL Guide, which was published in 2006, reiterates the main principles governing the creation or use of personal data processing (the rights and obligations of all parties and the formalities to be carried out).

■ shall not leave data on an in-house server or a server which is accessible by the general public (google, free, orange, …) or on another user's work station, unless he/she is authorised to do so by the authorised managers,

■ shall ensure the highest standards of politeness vis-à-vis his/her contacts in electronic exchanges either by e-mail or in chat-rooms…,

■ shall not state personal opinions which are unrelated to his/her professional activity and which may be detrimental to the CNRS,

■ shall ensure that he/she complies with legislation and, in particular that relating to offensive, racist, pornographic, defamatory publications.

The entity may not be held liable for the deterioration of information or for violations committed by a user who has failed to comply with these rules.

7.2 Electronic message application

The electronic message application is a work tool which is available for professional use.

■ All messages shall be deemed as being professional unless they specifically and explicitly mention their private nature on the subject line, or unless they are stored in a private data storage space.

■ All users shall organise and implement the means required to save messages which may be essential or simply useful as elements of proof.

■ It is forbidden to send classified data[3] unless specific provisions have been authorised, and so-called sensitive data should either not be sent or sent in encrypted form.

■ The user shall ensure that messages are only sent to the relevant recipients so as to avoid mass-mailing, the unnecessary clogging-up of the message application, and a reduction in service level.

► The permanent progression of IT technologies provides users with new services which may be accessed via their entities' network. Such new technologies, which may create a specific vulnerability risk, may only be used with the prior agreement of the entity's manager and in strict compliance with the information systems' security policy (CNRS' ISSP).

8. Analysis and verification of use of the resources

For the purposes of technical maintenance and management, verification for statistical purposes, tracking, optimisation, security or the detection of misuse, use of the IT resources and the Internet services, and exchanges via the network, may be analysed and verified in compliance with applicable legislation, in particular, the Act on information technology and civil liberties.

Users whose work stations are subject to remote maintenance shall be informed thereof beforehand.

Staff responsible for the verification work are subject to a non-disclosure obligation. Consequently, they may not disclose the information of which they become aware whilst carrying out their duties, in particular when such information is covered by secrecy of correspondence or relates to the user's private life, provided such information does not compromise either the due and proper technical operation of the applications, or their security, or the interest of the department.

9. Tracking

The CNRS is legally obliged to introduce a logging system of Internet access, the message application and exchanged data.

[3] This means classified defence data which covers "confidential defence", "secret defence" and "top secret defence" data.

Consequently, tracking tools are installed in all the information systems.

The CNRS has submitted a declaration to the CNIL mentioning, in particular, the period during which connection tracking and time records are kept, under the effective legislation.

10. Reminder of the main legal provisions

It is hereby reiterated that all the CNRS' officers, no matter what their status may be, are subject to effective French legislation and, in particular:

► the Act of 29 July 1881, as modified, on the freedom of the press,

► the Act no. 78-17 of 6 January 1978, as modified, on information technology, files and civil liberties,

► legislation relating to the corruption of the automated processing of data (Art. L 323-1 *et seq*. of the French Penal Code),

► the Act no. 94-665 of 4 August 1994, as modified, on the use of the French language,

► the Act no. 2004-575 on 21 June 2004 on confidence in the digital economy,

► the provisions of the French Intellectual Property Code on literary property and copyright.

11. Application

This charter applies to all officers of the CNRS' entities, no matter what their status may be and, more generally, to all persons, whether permanent or temporary [employees], who use, in any capacity whatsoever, the entity's IT resources and Internet services, and those which may be remotely accessed, either directly or in cascade mode, from the entity's network.

The persons referred to in the previous paragraph shall be informed of the charter by any and all means and, in particular:

- by a message sent on the message application when the user has an account, with the latter being obliged to represent that he/she has familiarised him/herself with this charter,

- by means of displaying in the entity's premises,

- by means of an appendix to the entity's by-laws,

- or by the supplying of a hard copy of the charter.

The charter may be appended to employment contracts and to procurement contract agreements, for which the performance requires access to the CNRS' IT resources and Internet services.

The charter is also available in English. Only the French version shall be deemed authentic.