



UNITÉ MIXTE DE RECHERCHE 1563 CNRS ECN ENSAG ENSAN

Règlement intérieur du laboratoire

20 JANVIER 2020

Préambule

Le laboratoire AAU « Ambiances Architectures Urbanités » est une Unité Mixte de Recherche du CNRS hébergée dans les locaux de l'École nationale supérieure d'architecture de Grenoble (ENSAG), de l'École nationale supérieure d'architecture de Nantes (ENSAN) et de l'École Centrale de Nantes (ECN). Il est désigné ci-après « l'Unité ».

Le présent règlement intérieur a été soumis à l'avis de l'Assemblée Générale du laboratoire réunie à Nantes le 17 janvier 2019.

Il s'applique à l'ensemble des membres de l'Unité, ainsi qu'aux étudiants, stagiaires, chercheurs invités et autres personnes qui participent à la vie du laboratoire sans être membres de l'Unité. Il est complémentaire à celui de l'ENSAG (équipe CRESSON), de l'ENSAN et de l'ECN (équipe CRENAU). En cas de contradiction, les dispositions les plus restrictives prévaudront.

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

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	4
Article 1. Organisation générale de l'Unité	4
1.1. Membres	4
1.2. Équipes	4
1.3. Direction	4
Article 2. Instances	5
2.1. Assemblée générale	5
2.2. Conseil de laboratoire	6
2.3. Comités de direction des équipes	7
Article 3. Locaux et système d'information	7
3.1. Accès aux locaux	7
3.2. Utilisation des moyens informatiques et sécurité du système d'information	8
Chapitre 2. Ressources humaines.....	8
Article 4. Durée du travail	8
Article 5. Horaires	8
5.1. Durée hebdomadaire de travail	8
Article 6. Congés	9
6.1. Congés annuels et RTT	9
6.2. Conditions d'octroi et d'utilisation	9
6.3. Journée de solidarité	9
6.4. Compte épargne temps (CET)	9
Article 7. Absences	9
7.1. Absence pour raison médicale	9
7.2. Autorisation d'absences et aménagement d'horaires	9
Article 8. Missions	10
Chapitre 3. Santé et sécurité.....	10
Article 9. Personnes ressources en matière de sécurité et de prévention des risques	10
9.1. Directeur d'Unité	10
9.2. Assistants de prévention	10
9.3. Modalités de concertation	10
9.4. Équipiers de sécurité incendie	10
Article 10. Organisation de la prévention au sein de l'Unité	11
10.1. Suivi médical des agents	11
10.2. Organisation des secours	11
10.3. Accident de service	11
10.4. Formation à la sécurité	11
10.5. Registres	11
10.6. Accueil de personnes extérieures	12
10.7. Travail isolé	12
Article 11. Interdictions	12
11.1. Animaux domestiques	12
11.2. Interdiction de fumer	12
11.3. Alcool	12

Chapitre 4. Diffusion de la recherche	13
Article 12. Confidentialité	13
Article 13. Propriété intellectuelle et obligation d'information	13
13.1. Propriété intellectuelle	13
13.2. Obligation d'informations du Directeur d'Unité	14
Article 14. Publications et communication	14
14.1. Formalisme des publications et communication	14
14.2. Logos et marques	14
14.3. Création de sites web	14
Article 15. Mise en œuvre de la Science ouverte	15
15.1. Ouverture des données de la recherche	15
15.2. Dépôt sur l'archive ouverte HAL	15
Chapitre 5. Dispositions générales	15
Article 16. Discipline	15
Article 17. Formation	15
17.1. Correspondant formation	15
17.2. Formation par la recherche	16
Article 18. Durée	16
Article 19. Publicité	16
ANNEXE N°1. Charte sur la sécurité du système d'information de l'Unité	18
ANNEXE N°2. Rôle et missions de l'assistant de prévention	25
ANNEXE N°3. Équippers de sécurité incendie	26
ANNEXE N°4. Note sur le travail isolé	27

Chapitre 1. Fonctionnement

Article 1. Organisation générale de l'Unité

1.1. Membres

L'Unité est composée de personnels de recherche et d'enseignement, de personnels d'appui et soutien à la recherche et de doctorants qui s'engagent dans la réalisation de son projet scientifique. Ceux-ci peuvent être membres permanents, membres contractuels ou membres associés.

Sont déclarés membres permanents les membres de l'Unité titulaires ou salariés en CDI exerçant dans les établissements tutelles de l'Unité, ou bien liés à l'Unité par une convention entre leur établissement employeur et l'un des établissements tutelles de l'Unité.

Sont déclarés membres contractuels les membres de l'Unité recrutés en CDD par l'un des établissements tutelles de l'Unité. Le statut de membre contractuel prend fin à l'échéance du contrat.

Sont déclarés membres associés les membres de l'Unité qui participent à la réalisation du projet scientifique de l'Unité sans avoir de lien contractuel avec ses établissements tutelles. Le statut de membre associé est accordé sur demande motivée auprès de l'une des équipes de l'Unité pour une durée de deux ans renouvelable.

L'Unité accueille de manière temporaire des étudiants, des stagiaires, des chercheurs invités qui n'en sont pas membres.

1.2. Équipes

L'Unité est organisée en deux équipes :

- L'équipe CRENAU, « Centre de Recherche Nantais Architectures Urbanités », située conjointement à l'École nationale supérieure d'architecture de Nantes et à l'École Centrale de Nantes,
- L'équipe CRESSON, « Centre de Recherche sur l'Espace Sonore et l'environnement urbain », située à l'École nationale supérieure d'architecture de Grenoble.

Chaque équipe est organisée en trois collèges :

- Le collège Recherche et enseignement,
- Le collège Appui et soutien à la recherche,
- Le collège Doctorants.

1.3. Direction

1.3.1. Directeur d'Unité et Directeurs d'équipes

L'Unité est dirigée par une Directrice ou un Directeur d'Unité, ci-après désigné « le DU », nommé par les tutelles après avis des instances compétentes des tutelles et du Conseil de laboratoire, pour assurer la direction scientifique, administrative et financière de l'unité pour la durée d'un programme pluriannuel. Lors du changement de programme pluriannuel, le principe d'alternance de la direction entre les équipes composant l'Unité est privilégié.

Chaque équipe est dirigée par une Directrice ou un Directeur d'équipe, ci-après désigné « le DE », également Directrice-Adjoint ou Directeur-Adjoint de l'Unité, élu parmi les membres de l'équipe.

Le DU et les DE forment le Collège de direction de l'Unité.

1.3.2. Élections internes pour proposer aux tutelles les noms de membres de l'Unité susceptibles d'assumer les fonctions de direction

À l'occasion du renouvellement pluriannuel, l'Unité s'organise pour proposer aux tutelles les noms de membres susceptibles d'assumer les fonctions de DU et de DE. Cette proposition fait l'objet d'un processus électoral interne.

La candidature à la fonction de DU peut être individuelle ou faire l'objet d'un « ticket » associant le nom du candidat à la fonction de DU et les noms des candidats à la fonction de DE de chaque équipe.

Si le DU élu s'est présenté sur un « ticket », alors les candidats du même « ticket » aux fonctions de DE sont également déclarés élus.

Si le DU élu s'est présenté de manière individuelle, alors des élections sont organisées au sein des équipes, dans un délai de deux mois, pour désigner les personnes qui seront proposées aux tutelles pour assumer les fonctions de DE.

1.3.3. Modalités du processus électoral interne

Les élections ont lieu au scrutin majoritaire à un tour à bulletin secret. Le vote par procuration est admis, à raison de deux procurations au plus par votant.

Les membres permanents et contractuels, ainsi que les doctorants, participent aux votes sous réserve d'être présents dans l'Unité depuis plus de 6 mois.

Les membres associés ne participent pas aux votes.

Le processus électoral commence par un appel à candidatures pour la fonction de DU lancé par le Conseil de laboratoire au moins deux mois avant la date prévue pour le vote. Les candidatures individuelles et par « ticket » sont reçues par le Conseil de laboratoire et diffusées à l'ensemble des membres de l'Unité au moins deux semaines avant la date prévue pour le vote.

Le cas échéant, les votes pour l'élection des DE dans les équipes suivent les mêmes modalités.

En cas de vacance d'un poste de DE, l'équipe concernée engage une procédure de désignation d'un nouveau DE pour la fin du mandat pluriannuel en cours.

Article 2. Instances

2.1. Assemblée générale

L'Assemblée Générale du laboratoire comprend tous les membres de l'Unité. Elle est réunie au moins une fois par an. La date de l'Assemblée Générale est annoncée à l'ensemble du laboratoire au moins trois semaines avant sa tenue.

L'ordre du jour est fixé par le Collège de direction. Il est transmis à l'ensemble du laboratoire en même temps que l'annonce de la date de l'Assemblée Générale.

Toute question particulière est inscrite à l'ordre du jour si la demande en a été faite par écrit auprès du Collège de direction au moins 10 jours avant la date fixée pour l'Assemblée Générale.

Les propositions débattues lors de l'Assemblée Générale peuvent être soumises au vote. Les votes ont lieu à main levée, sauf les votes sur les personnes, notamment les votes concernant la direction de l'Unité, qui ont lieu à bulletin secret.

Les membres permanents et contractuels de l'Unité, ainsi que les doctorants, participent aux votes sous réserve d'être présents dans l'Unité depuis plus de 6 mois. Les membres associés ne participent pas aux votes. Le vote par procuration est admis, à raison de deux procurations au plus par votant.

L'ordre du jour peut comporter un dernier point consacré aux questions diverses et qui ne donne lieu à aucun vote.

2.2. Conseil de laboratoire

2.2.1. Composition

En application de la décision n° 920368SOSI du 28 octobre 1992 modifiée relative à la constitution, la composition, la compétence et au fonctionnement des conseils de laboratoire des structures opérationnelles de recherche et des structures opérationnelles de service du CNRS, le Conseil de laboratoire de l'Unité se compose de 15 membres :

- 3 Membres de droit : le DU et les DE,
- 10 Membres élus : 3 représentants du collège Recherche et enseignement de chaque équipe (6 membres), 1 représentant du collège Appui et soutien à la recherche de chaque équipe (2 membres), 1 représentant du collège Doctorants de chaque équipe (2 membres),
- 2 Membres nommés par le Collège de direction parmi les membres de l'Unité.

La parité entre femmes et hommes est recherchée au sein du Conseil de laboratoire.

2.2.2. Compétences

Le Conseil de laboratoire a un rôle consultatif. Il est consulté par le DU 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 DU 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 DU, ainsi que des DE.

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 DU 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.

2.2.3. Fonctionnement

Le Conseil de laboratoire se réunit au moins trois fois par an, à l'initiative du DU, ou à la demande d'un tiers des membres du Conseil. Les séances peuvent se dérouler par visioconférence entre les sites des équipes de l'Unité. Le DU préside les séances.

Sept jours avant chaque séance, le DU adresse une convocation à chacun des membres du Conseil.

L'ordre du jour est fixé par le DU. L'inscription à l'ordre du jour d'une question particulière peut être demandée par un tiers au moins des membres du Conseil. Cette demande doit être formulée par écrit avant la date fixée pour la séance.

Tout ordre du jour relatif à une séance peut comporter un dernier point consacré aux questions diverses et qui ne donne lieu à aucun vote.

L'ordre du jour est porté à la connaissance de l'ensemble du laboratoire en même temps que la convocation.

Sur proposition du DU, le Conseil peut décider en début de séance d'ajouter un ou plusieurs points à l'ordre du jour. Le Conseil peut décider de modifier l'ordre des questions inscrites.

Les avis du Conseil sont adoptés à la majorité absolue, calculée sur le nombre total des membres présents ou représentés. Un vote ne peut avoir lieu que si le quorum, fixé à 8 membres présents ou représentés, est atteint.

Chaque membre du Conseil peut recevoir d'un seul membre absent une procuration écrite valable pour une seule séance et pour les points de l'ordre du jour portés sur la convocation.

Le Président du Conseil peut inviter toute personne dont il souhaite la présence à titre consultatif pour une séance et pour un point déterminé de l'ordre du jour.

Les votes ont lieu à main levée, sauf demande expresse de vote à bulletins secrets exprimée par un membre du Conseil. Les votes sur les personnes ont obligatoirement lieu à bulletins secrets.

A chaque séance, le Conseil désigne en son sein un secrétaire qui rédige le compte-rendu de la séance. Le compte-rendu de séance est soumis aux membres du Conseil pour approbation avant diffusion. Il est ensuite diffusé à l'ensemble des membres de l'Unité.

2.3. Comités de direction des équipes

Le DE de chaque équipe s'entoure d'un Comité de direction d'équipe dont les compétences concernent la vie de l'équipe, sa politique scientifique et les demandes d'association. En cas de désaccord, l'avis du Conseil de laboratoire prévaut sur l'avis des Comités de direction des équipes.

La parité entre femmes et hommes est recherchée au sein des Comités de direction des équipes.

Article 3. Locaux et système d'information

3.1. Accès aux locaux

Pour chaque équipe, l'accès aux locaux de l'Unité s'effectue en suivant les conditions d'accès définies par l'établissement hébergeur concerné.

La plage horaire de travail de référence est définie du lundi au vendredi, de 7h30 à 20h.

L'accès aux locaux en dehors de la plage horaire de travail de référence est expressément et nommément autorisé par le DU en accord avec l'établissement hébergeur.

Les personnes non concernées par les activités de l'Unité ne peuvent avoir accès aux locaux sans l'autorisation du DU, en dehors des cas prévus par la réglementation 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...) à l'établissement hébergeur concerné.

3.2. Utilisation des moyens informatiques et sécurité du système d'information

L'utilisation des moyens informatiques de l'Unité est soumise aux dispositions de la Charte sur la sécurité du système d'information (SI) de l'Unité qui figure en annexe n°1 du présent règlement.

Les conditions d'accès au SI de l'Unité sont définies dans cette Charte. En tout état de cause les personnes non concernées par les activités de l'Unité ne peuvent avoir accès au système d'information de l'Unité sans l'autorisation du DU.

La Charte sur la sécurité du système d'information de l'Unité, qui a notamment pour objet de préciser la responsabilité des utilisateurs au regard de la législation, doit être signée par tout nouvel arrivant (voir annexe n°1, déclaration sur l'honneur).

Chapitre 2. Ressources humaines

Article 4. 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, la durée annuelle de travail est fixée à 1 607 heures. Cette durée tient compte des 7 heures de travail dues au titre de la journée de solidarité (cf. article 6.3).

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.

Article 5. Horaires

5.1. 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 réglementaires 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.

5.1.1. Pour les agents du CNRS

La durée hebdomadaire de travail des agents CNRS est fixée, pour un temps plein, à 38h30.

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.

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.

Mise en œuvre du télétravail au CNRS (Documents de référence : loi n°2012-347 du 12 mars 2012 ; décret n°2016-151 du 11 février 2016 relatif aux conditions et aux modalités de mise en œuvre du télétravail dans la fonction publique ; Guide opérationnel du télétravail, octobre 2018).

Article 6. Congés

6.1. 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 réglementaires telles que définies par l'employeur de l'agent.

6.2. Conditions d'octroi et d'utilisation

6.2.1. Conditions d'octroi

L'octroi des congés fait nécessairement l'objet d'une demande préalable auprès du DE de l'équipe à laquelle l'agent appartient. Un délai de prévenance de 7 jours doit être respecté.

Les agents du CNRS déposent leurs demandes d'absences via l'outil AGATE.

Les congés sont accordés sous réserve des nécessités du service.

6.2.2. Conditions d'utilisation

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

Le report des jours de congés annuels et des jours RTT non utilisés pendant l'année civile est autorisé selon les dispositions prévues par l'employeur de l'agent.

Le suivi des congés (annuels et RTT) est réalisé dans l'Unité sous la responsabilité des DE.

Pour les agents CNRS, ce suivi est réalisé via l'outil AGATE.

6.3. 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 définie par leur établissement employeur.

6.4. Compte épargne temps (CET)

Les conditions d'alimentation et d'utilisation du CET sont fixées par chaque établissement employeur des différents personnels de l'Unité.

Pour les agents CNRS la gestion du CET (alimentation, utilisation...) est réalisée via l'outil AGATE.

Article 7. Absences

7.1. Absence pour raison médicale

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

7.2. Autorisation d'absences et aménagement d'horaires

Les modalités d'autorisation d'absences et d'aménagement d'horaires sont fixées par chaque établissement employeur des différents personnels de l'Unité.

Article 8. Missions

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 DU ou par l'établissement employeur de l'agent. Ce document assure notamment la couverture de l'agent au regard de la réglementation sur les accidents de service.

La réglementation impose l'autorisation préalable du fonctionnaire sécurité défense pour les missions des agents CNRS dans certains pays étrangers.

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

Dans l'hypothèse où l'agent utilise un véhicule administratif ou son véhicule personnel, le DU ou le DE concerné doit avoir donné préalablement son autorisation.

Chapitre 3. Santé et sécurité

Article 9. Personnes ressources en matière de sécurité et de prévention des risques

9.1. Directeur d'Unité

Il lui incombe de veiller à la santé et à la sécurité des agents placés sous son autorité et d'assurer la sauvegarde des biens dont il dispose, en lien avec les établissements hébergeurs.

Il nomme, après avis du Conseil de laboratoire, un (ou plusieurs) Agent(s) de Prévention (AP), placé(s) sous son autorité qui l'assiste(nt) et le conseille(nt) dans le domaine de la prévention et de la sécurité.

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

9.2. Assistants de prévention

L'assistant de prévention a pour mission de conseiller le DU dans la démarche d'évaluation des risques, la mise en place d'une politique de prévention ainsi que sur la mise en œuvre des règles d'hygiène et de sécurité dans l'Unité (cf. annexe n°2).

Les noms des assistants de prévention figurent à l'organigramme de l'Unité.

9.3. Modalités de concertation

Les problématiques relevant de la santé et de la sécurité au travail devront être traitées au moins une fois par an au sein du conseil d'Unité. Dans ce cas, les AP sont invités à y participer.

Les CHSCT des établissements de tutelle sont informés des questions d'hygiène et de sécurité traitées au sein de cette instance.

9.4. Équippers de sécurité incendie

Voir annexe n°3 du présent règlement.

Article 10. Organisation de la prévention au sein de l'Unité

10.1. 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 DU doit veiller à ce que chaque agent de l'Unité se présente aux convocations du service de médecine de prévention.

Les noms et coordonnées des médecins de prévention sont disponibles auprès des établissements employeurs des différents personnels.

10.2. Organisation des secours

Les consignes d'évacuation en cas d'urgence sont indiquées par les établissements hébergeurs.

Tous les membres de l'Unité sont tenus de participer aux exercices d'évacuation organisés par les établissements hébergeurs.

10.3. Accident de service

Le DU doit immédiatement être informé de tout accident de service, de trajet ou de mission d'agent travaillant dans l'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 selon les règles définies par l'établissement employeur de l'agent.

10.4. Formation à la sécurité

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

La formation des nouveaux entrants est assurée dans chaque équipe par les Assistants de Prévention. Lors de leur arrivée, les nouveaux entrants sont convoqués à une réunion d'accueil au cours de laquelle l'Assistant de Prévention présente les règles de sécurité relatives à l'équipe et les outils mis à disposition des agents.

10.5. 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.

- Emplacement de ce registre pour l'équipe CRENAU : espace de convivialité, étage 1.
- Emplacement de ce registre pour l'équipe CRESSON : bureau n°256 (David ARGOUD).

Un registre de signalement de danger grave et imminent, ouvert au timbre du CHSCT compétent, doit être mis à la disposition des agents : le DU et le DE concerné doivent porter à la connaissance des agents l'emplacement de ce registre dans l'établissement, et s'il y a lieu, en mettre un à disposition. Pour le CNRS, ce registre se trouve dans le bureau de l'Ingénieur régional de prévention et de sécurité à la délégation régionale Bretagne et Pays de la Loire (DR17) et dans le bureau de l'Assistante de direction à la délégation régionale Alpes (DR11). Pour les autres établissements tutelles, ce registre se situe dans le bureau de l'Assistant de Prévention de l'établissement.

10.6. Accueil de personnes extérieures

10.6.1. Stagiaires et visiteurs

L'accueil de stagiaires et de visiteurs est encadré par une convention passée avec l'établissement hébergeur de l'équipe concernée.

10.6.2. Entreprises extérieures

Lors de l'intervention d'entreprises extérieures dans l'Unité, une visite de prévention et, s'il y a lieu, un plan de prévention doit être réalisé par l'Assistant de Prévention de l'équipe concernée en concertation avec l'Assistant de Prévention de l'établissement hébergeur.

10.7. Travail isolé

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

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

- Pour l'équipe grenobloise, la plage horaire de travail de référence correspond à la plage horaire d'ouverture de l'ENSAG. L'accord du DE et celui de la direction de l'ENSAG sont requis pour tout accès aux locaux du laboratoire en dehors de la plage horaire d'ouverture de l'ENSAG.
- Pour l'équipe nantaise, une autorisation de présence en dehors de la plage de travail de référence peut être donnée par le DE à titre dérogatoire pour un ensemble de travaux définis dans une note interne diffusée à l'ensemble des membres de l'équipe et remise aux nouveaux arrivants.

Les temps de présence en dehors de la plage de travail de référence ne peut être motivé pour des raisons de convenance personnelle.

Dans le cas où des travaux dangereux doivent nécessairement être exécutés hors des horaires normaux et/ou sur des lieux isolés ou locaux éloignés, il est obligatoire d'être accompagné ou de mettre en œuvre des mesures compensatoires appropriées.

La note CNRS en date du 30 juin 2010 indique la position du CNRS sur le travail isolé et propose des dispositions et des recommandations relatives à cette problématique (voir note en annexe n°4).

Article 11. Interdictions

11.1. Animaux domestiques

L'introduction d'animaux domestiques dans les locaux est strictement interdite, sauf situations prévues par la législation.

11.2. 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.

11.3. 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 DU.

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

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

Chapitre 4. Diffusion de la recherche

Article 12. Confidentialité

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

Par conséquent, les personnels de l'Unité sont tenus de respecter la confidentialité de toutes les informations de nature scientifique, technique ou autre, quel qu'en soit le support, ainsi que de tous les produits, échantillons, composés, matériels biologiques, appareillages, systèmes logiciels, méthodologies et savoir-faire ou tout autre élément ne faisant pas partie du domaine public dont ils pourront avoir connaissance du fait de leur séjour au sein de l'Unité, des travaux qui leur sont confiés ainsi que de ceux de leurs collègues.

Cette obligation de confidentialité reste en vigueur tant que ces informations ne sont pas dans le domaine public.

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

Pour toute présentation et tout échange sur les travaux et résultats de recherche de l'Unité avec des partenaires publics et/ou privés, la signature d'un accord de secret entre les parties concernées est fortement recommandée. Les structures de valorisation des établissements de tutelle peuvent être utilement contactées à cet effet.

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

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

Article 13. Propriété intellectuelle et obligation d'information

13.1. 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.

13.2. Obligation d'informations du Directeur d'Unité

Le personnel doit informer le DU et le DE concerné de tout projet de collaboration avec des partenaires publics ou privés, en particulier des projets de collaboration internationale qui nécessitent avant signature l'autorisation formelle du ministère de tutelle.

Un exemplaire de tout contrat doit être remis au DU et au DE concerné après sa signature.

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

Article 14. Publications et communication

14.1. 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 suivantes :

- Nom et prénom de(s) l'auteur(s)
- Employeur des auteurs
- Intitulé du laboratoire et de l'équipe
- Tutelle(s) de l'Unité

Un modèle de présentation de l'affiliation est défini dans chaque équipe, selon le contexte du site.

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 à la personne chargée des ressources documentaires au sein de l'équipe.

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.

14.2. Logos et marques

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

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

14.3. Création de sites web

Le site internet de l'Unité est publié à l'adresse : <https://aau.archi.fr>

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

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 Collège de direction.

Il est rappelé que le DU 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 DU. 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 de l'Unité, doit respecter la charte graphique de l'Unité disponible à l'adresse : <http://aau.archi.fr/resources/>

Article 15. Mise en œuvre de la Science ouverte

15.1. Ouverture des données de la recherche

L'Unité s'engage en faveur du mouvement de la Science ouverte. Elle favorise l'ouverture et le partage des données de la recherche en suivant la ligne directrice de la Commission européenne "*as open as possible, as closed as necessary*", et encourage la rédaction des plans de gestion de données et l'archivage des données selon les principes FAIR (*Findable, Accessible, Interoperable, Reusable*).

15.2. Dépôt sur l'archive ouverte HAL

Toute publication issue de l'Unité doit faire l'objet d'un dépôt sur l'archive ouverte HAL. Ce dépôt est réalisé par l'un des auteurs de la publication en accord avec l'ensemble de ses coauteurs. Le dépôt en texte intégral est encouragé chaque fois que possible (cf. l'article 30 de la Loi pour une République Numérique).

Chapitre 5. Dispositions générales

Article 16. 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 autres établissements tutelles de l'Unité, les sanctions disciplinaires sont prises en application des règles régissant chaque corps ou statuts de personnels.

Article 17. Formation

17.1. Correspondant formation

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

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

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

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

17.2. Formation par la recherche

L'encadrement des stagiaires par un agent titulaire ou non de l'Unité est soumis à l'autorisation préalable du DU ou du DE concerné. 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'École doctorale de rattachement.

Article 18. Durée

Le règlement intérieur entre en vigueur à la date de signature par le Délégué Régional du CNRS et des représentants dûment habilités des autres tutelles. Il annule et remplace le précédent règlement intérieur du laboratoire daté de mai 2009.

Il peut être modifié lors du changement de DU, 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 DU, le présent règlement intérieur et ses annexes lui sont remis par le Délégué Régional du CNRS.

Article 19. Publicité

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

Il est ensuite consultable sur le site internet de l'Unité.

Fait à Nantes, le 20 janvier 2020

Signature des représentants légaux des tutelles

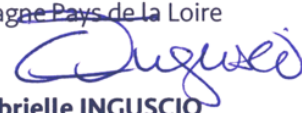
Pour le CNRS

Délégation régionale
**Pour le délégué régional empêché,
Alpes et par délégation**


L'adjoint au délégué régional
Jérôme PARET
Délégué régional

Pour le CNRS

Délégation régionale
Bretagne Pays de la Loire


Gabrielle INGUSCIO
Déléguée régionale

Pour l'École Centrale de
Nantes



Pour l'ENSA Grenoble


Marie WOZNIAK
Directrice



Visa du Directeur de l'Unité


Daniel SIRET

ANNEXE N°1. Charte sur la sécurité du système d'information de l'Unité

a) Préambule

Le « système d'information » de l'Unité recouvre l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunication locaux, ainsi que celles auxquelles il est possible d'accéder à distance ou en cascade à partir du réseau de l'Unité. L'informatique nomade, tels que les assistants personnels, les ordinateurs portables, les téléphones portables... est également un des éléments constitutifs du système d'information.

Le terme « utilisateur » recouvre toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut. Il s'agit notamment de :

- tout agent titulaire ou non titulaire concourant à l'exécution des missions du service public de l'enseignement et de la recherche ;
- tout prestataire ayant contracté avec l'Unité. Le contrat devra prévoir expressément l'obligation de respect de la présente Charte.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

La présente Charte, associée au règlement intérieur de l'Unité, a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation, afin d'instaurer un usage conforme des ressources d'informations et des services Internet relevant des établissements tutelles de l'Unité. Ces ressources et services constituent un élément important du patrimoine scientifique et technique de l'Unité.

La présente Charte doit être signée par tout nouvel arrivant (déclaration sur l'honneur ci-après).

Engagements de l'Unité

L'Unité porte à la connaissance de l'utilisateur la présente Charte.

L'Unité met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs.

L'Unité facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'Unité est tenue de respecter l'utilisation résiduelle du système d'information à titre privé.

En adhérant au réseau RENATER, les écoles d'architecture tutelles de l'Unité se sont engagées à respecter une charte d'usage et de sécurité, propre aux membres de ce réseau. Le directeur d'établissement a désigné auprès de RENATER un administrateur de site, responsable de la mise en œuvre et de la gestion du réseau. A ce titre, il doit notamment s'assurer que l'usage des ressources informatiques pour accéder à l'internet se fait conformément aux prescriptions et aux recommandations formulées par les gestionnaires du réseau RENATER.

En conséquence et afin de satisfaire ces exigences, les règles et les obligations définies dans la présente Charte s'appliquent à tout usager des moyens informatiques de l'école ainsi que des ressources extérieures accessibles via les divers réseaux informatiques, notamment les divers outils interactifs du réseau @aau.archi.fr, @crenau.archi.fr, @grenoble.archi.fr, @nantes.archi.fr.

Engagements de l'utilisateur

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

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

L'utilisation des ressources qui sont mises à sa disposition doit être rationnelle et loyale afin d'en éviter la saturation ou le détournement à des fins personnelles.

b) Champ d'application

Les règles d'usage et de sécurité figurant dans la présente Charte s'appliquent à l'Unité ainsi qu'à l'ensemble de ses membres.

Ces règles s'appliquent à toute personne autorisée à utiliser les moyens informatiques de l'Unité, y compris les moyens informatiques mutualisés ou externalisés, et s'étendent aux réseaux extérieurs accessibles par l'intermédiaire des réseaux des établissements tutelles de l'Unité.

c) Conditions d'utilisation du système d'information

Utilisation professionnelle / privée

Le système d'information de l'Unité est un ensemble d'outils de travail (serveurs, messagerie, internet...) ouverts à des usages professionnels administratifs, pédagogiques et de recherche. Il peut également constituer le support d'une communication privée dans les conditions décrites ci-dessous.

L'utilisation résiduelle du système d'information à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation. Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.

Toute information est réputée 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 de ses données à caractère privé dans un espace de données prévu explicitement¹ à cet effet ou en mentionnant le caractère privé sur la ressource². La protection et la sauvegarde régulière des données à caractère privé incombent à l'utilisateur.

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif de l'Unité ou de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'établissement ne pouvant être engagée quant à la conservation de cet espace. Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de l'Unité.

L'utilisation du système d'information à titre privé doit respecter la réglementation en vigueur. En particulier, la détention, diffusion et exportation d'images à caractère pédophile³, ou la diffusion de contenus à caractère raciste ou antisémite⁴ est totalement interdite. Par ailleurs, eu égard à la mission de l'Unité, la consultation de sites de contenus à caractère pornographique depuis les locaux de l'Unité hors contexte professionnel est interdite.

Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition.

d) Principes de sécurité

Règles de sécurité applicables

Les établissements hébergeurs de l'Unité et l'Unité mettent en œuvre les mécanismes de protection appropriés sur le système d'information mis à la disposition des utilisateurs. L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

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

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ; chaque utilisateur est responsable de l'utilisation qui en est faite ;
- de garder strictement confidentiels son ou ses codes d'accès et ne pas les dévoiler à un tiers ;

¹ Pour exemple, cet espace pourrait être dénommé « _privé_ ».

² Pour exemple, « _privé_nom_de_l_objet_ » : l'objet étant un message, un fichier ou toute autre ressource numérique.

³ Article L 323-1 et s. du Code pénal.

⁴ Article 24 et 26bis de la Loi du 29 juillet 1881.

- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître ;
- de veiller à ne pas laisser son poste de travail en libre accès.

Les mots de passe seront choisis pour être difficiles à deviner.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

De la part de l'Unité :

- veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie ;
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.

De la part de l'utilisateur :

- s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'Unité, à moins de faire une demande préalable auprès de l'administrateur qui procédera au contrôle de celui-ci (système à jour, antivirus à jour...) afin de s'assurer qu'il n'y ait pas d'effets néfastes sur le système informatique de l'Unité et de l'établissement hébergeur ;
- ne pas installer, télécharger ou utiliser sur le matériel de l'Unité des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de sa hiérarchie ;
- se conformer aux dispositifs mis en place par l'Unité pour lutter contre les virus et les attaques par programmes informatiques ;
- s'engager à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou du logiciel ;
- veiller à protéger les matériels mis à sa disposition contre le vol et les dégradations ;
- appliquer les recommandations sécurité de l'Unité.

Devoirs de signalement et d'information

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

Mesures de contrôle de la sécurité

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'Unité se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- qu'une maintenance à distance est précédée d'une information de l'utilisateur ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée, et le cas échéant supprimée.

Les établissements hébergeurs de l'Unité et l'Unité informent l'utilisateur que le système d'information peut donner lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Les personnels chargés des opérations de contrôle du système d'information sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur.

En revanche, ils doivent communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité, ou si elles tombent dans le champ de l'article 40 alinéa 2 du code de procédure pénale⁵.

⁵ Obligation faite à tout fonctionnaire d'informer sans délai le procureur de la République de tout crime et délit dont il a connaissance dans l'exercice de ses fonctions.

e) Communication électronique

Messagerie électronique

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

Adresses électroniques

L'Unité s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative⁶ lui permettant d'émettre et de recevoir des messages électroniques. L'utilisation de cette adresse nominative est ensuite de la responsabilité de l'utilisateur.

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

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'Unité.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'utilisateurs, relève de la responsabilité exclusive de l'Unité. Ces listes ne peuvent être utilisées sans autorisation explicite.

Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé⁷ ou s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place. Dans ce cas, les termes en sont précisés et portés à la connaissance de l'utilisateur par le fournisseur de service de messagerie.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques...).

Les échanges électroniques (courriers, forums de discussion, etc.) se doivent de respecter la correction normalement attendue dans tout type d'échange tant écrit qu'oral.

La transmission de données classifiées⁸ est interdite sauf dispositif spécifique agréé. La transmission de données dites sensibles doit être évitée ou effectuée sous forme chiffrée.

Émission et réception des messages

L'utilisateur doit faire preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d'escroquerie, chaînes...).

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

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

Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles 1369-1 à 1369-11 du code civil⁹.

L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

⁶ Par exemple, l'adresse est de la forme : prenom.nom@<nom de domaine institutionnel>.fr

⁷ Pour exemple, les messages comportant le terme « privé » dans l'objet ou sujet du message.

⁸ Il s'agit des données classifiées de défense qui couvre le « confidentiel défense », le « secret défense » et le « très secret défense ».

⁹ Issus de la loi n° 2004-575 du 21 juin 2004, ces articles fixent certaines obligations pour la conclusion des contrats en ligne.

Stockage et archivage des messages

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.

Internet

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'Unité.

Internet est un outil de travail ouvert à des usages professionnels (administratifs, pédagogiques et de recherche). Si une utilisation résiduelle privée, telle que définie en section c), peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'administration sont présumées avoir un caractère professionnel. L'administration peut les rechercher aux fins de les identifier.

Publication sur les sites internet et intranet de l'Unité

Toute publication d'information sur les sites internet ou intranet de l'Unité¹⁰ doit être validée par un responsable de site ou responsable de publication nommément désigné.

Aucune publication d'information à caractère privé (pages privées...) sur les ressources du système d'information de l'Unité n'est autorisée, sauf disposition particulière précisée dans un guide d'utilisation établi par le service ou l'établissement.

Sécurité

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

Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'Unité. Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou l'établissement.

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

Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article g) de la présente Charte.

L'Unité se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité du système d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'Unité, codes malveillants, programmes espions...).

f) Traçabilité

L'Unité est dans l'obligation légale de mettre en place un système de journalisation¹¹ des accès Internet, de la messagerie et des données échangées.

L'Unité se réserve le droit de mettre en place des outils de traçabilité sur le système d'information.

Préalablement à cette mise en place, l'Unité procèdera, auprès de la Commission nationale de l'informatique et des libertés, à une déclaration, qui mentionnera notamment la durée de conservation des traces et durées de connexions, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n° 78-17 du 6 janvier 1978 modifiée.

g) Respect de la propriété intellectuelle

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

En conséquence, chaque utilisateur doit :

¹⁰ A partir des ressources informatiques mises à la disposition de l'utilisateur.

¹¹ Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur.

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, 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.

h) Respect de la loi Informatique et Libertés, LCEN et RGPD

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi Informatique & Libertés n° 78-17 du 6 janvier 1978 modifiée, ainsi que la loi pour la Confiance dans l'Économie Numérique (LCEN) n° 2004-575 du 21 juin 2004, ainsi que le Règlement Général sur la Protection des Données (RGPD), n° 2016/679 du 27 avril 2016.

Le Règlement Général sur la Protection des Données (RGPD) n° 2016/679 est devenu applicable dans l'union européenne depuis le 25 mai 2018.

Les données à caractère personnel sont des informations qui permettent – sous quelque forme que ce soit – directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

Toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par les lois Informatique et Libertés, LCEN et RGPD.

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement les services compétents qui prendront les mesures nécessaires au respect des dispositions légales.

Tout traitement de données à caractère personnel doit être déclaré préalablement à sa mise en œuvre auprès du Correspondant Informatique et Libertés (CIL) désigné par l'établissement à la Commission Nationale Informatique et Libertés.

Par ailleurs, conformément aux dispositions de ces lois, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation du système d'Information.

i) Limitation des usages

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

Par « personne juridiquement responsable », il faut entendre toute personne ayant la capacité de représenter l'Unité (directeur, chef d'établissement...).

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

j) Entrée en vigueur de la Charte

La présente Charte annule et remplace tous les autres documents relatifs à l'utilisation du système d'information de l'Unité, sans pour autant se substituer aux chartes ou règlements intérieurs des établissements hébergeurs ainsi qu'à la charte du CNRS.

DÉCLARATION SUR L'HONNEUR

Feuille à détacher et à retourner au responsable informatique de l'équipe concernée

Nom : _____ Prénom : _____

☐ Administratif ☐ Enseignant ☐ Étudiant ☐ Autre, préciser : _____

Je déclare avoir pris connaissance de la Charte sur la sécurité du système d'information de l'UMR CNRS 1563 AAU, j'en accepte tous les termes et je m'engage à les respecter.

Je souhaite rediriger mon courrier électronique vers ma boîte personnelle : ☐ OUI ☐ NON

Si oui, indiquer votre adresse de messagerie personnelle :

Je souhaite utiliser mon équipement informatique personnel : ☐ OUI ☐ NON

Si oui, je m'engage à donner à l'administrateur de l'équipe un droit de contrôle de sécurité (utilisation de logiciels ne nécessitant pas d'installation).

Fait à : _____ Le (date) : _____

Signature

Précédée de la mention manuscrite « lu et approuvé »

Pour l'équipe CRESSON

Votre nom d'utilisateur pour l'ouverture d'une session sur un ordinateur et pour la messagerie sera de la forme : nom.p où p est l'initiale du prénom.

Votre courriel sera de la forme :
nom.p@grenoble.archi.fr

et
prenom.nom@grenoble.archi.fr

Mot de passe à définir.

Pour l'équipe CRENAU

Votre nom d'utilisateur pour l'ouverture d'une session sur un ordinateur sera de la forme :
pnom où p est l'initiale du prénom.

Votre courriel sera de la forme :
prenom.nom@crenau.archi.fr

Les mots de passe provisoires pour l'ouverture de session ainsi que le courriel vous seront remis à votre arrivée par le responsable informatique de l'équipe.

ANNEXE N°2. Rôle et missions de l'assistant de prévention

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

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

L'AP figure à l'organigramme fonctionnel de l'Unité.

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

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

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

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

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

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

Il anime le groupe de travail chargé de l'évaluation des risques professionnels.

Il veille à la mise en place des premiers secours en cas d'accident, et d'une équipe de première intervention spécialisée en cas de risques spécifiques.

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

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

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

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

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

ANNEXE N°3. Équipers de sécurité incendie

Pour l'équipe nantaise :

- Équipier de 1ère intervention : Véronique DOM, niveau 1 du laboratoire, bureau façade Ouest.
- Chargés d'évacuation :
 - Guide-file : Laurent CHARRIEU, niveau 1 du laboratoire, bureau façade Ouest.
 - Serre-file : Laurence BIZIEN, niveau 2 du laboratoire, bureau façade Nord.

Pour l'équipe grenobloise :

- Chargés d'évacuation :
 - Guide-file : Françoise ACQUIER, bureau 279.
 - Serre-file : David ARGOUD, bureau n°256.
 - Serre-file : Jul MC OISANS, bureau n°255.

ANNEXE N°4. Note sur le travail isolé

Paris, le 30 juin 2010

Le Directeur général
Délégué aux ressources



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, ACO, ...).

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 œuvre 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** (nourissage 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).