CONSEIL D'ADMINISTRATION
DELIBERATION N° 2019-06-28-08

DELIBERATION DU CONSEIL D'ADMINISTRATION DE L'UNIVERSITE CLERMONT AUVERGNE PORTANT SUR LA MISE EN PLACE DU TELETRAVAIL A COMPTER DU 1ER SEPTEMBRE 2019 A L'UCA

LE CONSEIL D'ADMINISTRATION DE L'UNIVERSITE CLERMONT AUVERGNE, EN SA SEANCE DU 28 JUIN 2019,

Vu le code de l'Education ;
Vu les statuts de l'Université Clermont Auvergne **;**
Vu l'avis du comité technique de l'UCA en date du 25 juin 2019 ;

PRESENTATION DU PROJET
L'objectif de cette délibération vise à mettre en place le télétravail à compter du 1er septembre 2019 à l'Université Clermont Auvergne.

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

Après en avoir délibéré ;

DECIDE

La mise en place du télétravail à compter du 1er septembre 2019 à l'UCA, dans les conditions telles que prévues en annexe.

Membres en exercice : 37
Votes : 24
Pour : 24
Contre : 0
Abstentions: 0

Le Président,

Mathias BERNARD

CLASSE AU REGISTRE DES ACTES SOUS LA REFERENCE : CA UCA 2019-06-28-08

TRANSMIS AU RECTEUR :

PUBLIE LE :

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

UNIVERSITÉ Clermont Auvergne

CHARTE DU TELETRAVAIL A l'UCA

Le décret n° 2016-151 du 11 février 2016 fixe les conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature. L'arrêté du 3 novembre 2017 porte application de ce décret au ministère de l'enseignement supérieur, de la recherche et de l'innovation.
Le télétravail est un mode d'organisation du travail dont l'objectif est triple :

- Mieux articuler vie personnelle et vie professionnelle,
- Améliorer la qualité du travail,
- Participer à une démarche éco-responsable en réduisant les déplacements domicile-travail.

Le télétravail désigne toute forme d'organisation du travail dans laquelle les fonctions, qui auraient pu être exercées par un agent dans les locaux de son employeur, sont réalisées hors de ces locaux de façon régulière et volontaire en utilisant les technologies de l'information et de la communication.
Ne sont pas considérées comme du télétravail les périodes d'astreintes mentionnées à l'article 5 du décret du 25 août 2000 relatif à l'aménagement et à la réduction du temps de travail dans la fonction publique de l'Etat et dans la magistrature.
Les présentes lignes directrices ont pour objet de préciser les modalités d'application du télétravail à l'UCA.

I. Le champ d'application du télétravail

A. Les bénéficiaires

Le télétravail est ouvert aux agent BIATSS de l'UCA, fonctionnaires (titulaires et stagiaires) ou agents contractuels, ayant acquis 6 mois d'ancienneté dans l'établissement et sur leur poste.

B. Les activités éligibles

Par principe aucun agent n'est exclu du télétravail. L'inéligibilité de certaines activités au télétravail, si celles-ci ne constituent pas la totalité des activités exercées par l'agent, ne s'oppose pas à la possibilité pour l'agent d'accéder au télétravail dès lors qu'un volume suffisant d'activités en télétravail peut être identifié et regroupé au minimum sur une journée.

Sont considérées comme éligibles au télétravail les activités autres que celles qui répondent à l'un des critères suivants :
- la nécessité d'assurer un accueil ou une présence physique sur son lieu d'affectation auprès de tiers (agents, usagers, élèves, étudiants, apprentis, stagiaires…), activités nécessitant la présence pour garantir l'entretien des bâtiments et du mobilier ou en raison des équipements matériels spécifiques nécessaires à l'exercice de l'activité ou des soins à apporter à des animaux ;
- les activités se déroulant par nature en dehors de son lieu d'affectation (mission sur le terrain) ;
- l'accomplissement de travaux nécessitant l'utilisation de logiciels ou applications dont la sécurité ne peut être garantie en dehors du lieu d'affectation ;
- le traitement de données confidentielles ou à caractère sensible, dès lors que le respect de la confidentialité de ces données ne peut être assuré en dehors du lieu d'affectation.

C. Le lieu de télétravail
Le télétravail s'exerce au domicile de l'agent.

D. La quotité de télétravail
La quotité des fonctions pouvant être exercées sous la forme du télétravail ne peut être supérieure à deux jours par semaine.
Le temps de présence sur le lieu d'affectation ne peut être inférieur à trois jours par semaine.
Les jours de télétravail sont des journées complètes et ne peuvent pas être découpés en ½ journée.
Chaque jour de la semaine peut être un jour de télétravail, y compris la journée contractée (pour les agents concernés).

En ce qui concerne les agents à temps partiel, les agents travaillant à moins de 80% ne sont pas éligibles au télétravail. Les agents travaillant à 80 ou 90% peuvent télétravailler une journée par semaine.

Le seuil de présence minimale dans le service est aussi applicable aux agents bénéficiant de décharges syndicales partielles.

Dans la mesure du possible, il conviendra de privilégier les réunions par téléphone, visioconférence ou tout autre moyen permettant à l'agent d'y participer à distance dans de bonnes conditions.

L'agent et le n+1 veillent à l'équilibre de l'amplitude horaire entre jours sur site et jours télétravaillés.

Toutefois, afin de préserver une souplesse d'organisation, il pourra être demandé à l'agent, de manière occasionnelle et justifiée par l'activité de l'équipe ou du service, de revenir sur site un jour normalement télétravaillé, sans que cette journée non télétravaillée ait vocation à être reportée (exemples : pic temporaire d'activité, urgence nécessitant une présence physique, participation à une réunion, ...).
Les jours télétravaillés n'ouvrent pas droit à la possibilité de report y compris les jours fériés ou de fermeture du service ou d'autorisations d'absence.

E. La formation
L'UCA s'engage à mettre en œuvre des formations relatives au cadre général, à la mise en place et à la gestion du télétravail (règles de fonctionnement, santé et sécurité…) ainsi qu'aux risques et contraintes du télétravail. Ces formations seront obligatoires pour les agents et les encadrants avant la mise en place du télétravail.
1. Des agents
Tout agent qui est autorisé à télétravailler bénéficiera d'une formation sur les équipements mis à sa disposition et sur les caractéristiques de ce mode d'organisation du travail.
2. Des encadrants
Des actions de formation spécifiques seront organisées pour tout encadrant dont des agents télétravaillent. Elles porteront sur les spécificités du management à distance et notamment la cohésion d'équipe et la continuité de service.

F. Le suivi de l'activité en télétravail
Le télétravail fait l'objet d'un bilan annuel présenté au CHSCT et au CT.
A cette occasion le présent document pourra être révisé après avis du CHSCT et du CT.
Dans le bilan social de l'UCA, une rubrique « télétravail » sera proposée (nombre de télétravailleurs par corps, genres, statuts, jours de la semaine choisis pour le télétravail, lieu du télétravail, lieu d'affectation, nombre de jours télétravaillés par semaine, nombre de demandes acceptées et

refusées, problèmes rencontrés par les télétravailleurs et les responsables, améliorations et changements positifs observés dans le travail, etc.).
Le service de gestion des personnels BIATSS à la DRH est chargé de ce suivi, de la présentation en CHSCT et CT.

II. La procédure d'autorisation

A. La demande de l'agent

Le télétravail est basé sur le volontariat. Il ne peut pas être imposé à l'agent.

L'exercice des fonctions en télétravail est accordé sur demande écrite de l'agent adressée à son n+1, après validation par le directeur de la structure (responsable administratif, directeur d'unité, directeur de service central).
La demande est formalisée par le formulaire en annexe 1.

La demande de l'agent précise les modalités d'organisation souhaitées, notamment les jours télétravaillés, ainsi que le lieu d'exercice du télétravail. Le supérieur apprécie la compatibilité de la demande avec la nature des activités exercées et l'intérêt du service après un entretien avec l'agent.

Cette demande est faite dans le cadre d'une campagne annuelle (mai-juin). Elle peut cependant être formulée également au fil de l'eau. La campagne annuelle est lancée au moment des entretiens professionnels. Lors de son entretien professionnel, l'agent pourra indiquer qu'il souhaite faire une demande de télétravail.
La demande de l'agent est transmise également, pour information à la DRH.

En cas de mobilité sur un autre poste, l'agent doit présenter une nouvelle demande. L'ancienneté de 6 mois sur le poste sera à apprécier entre le responsable et l'agent, selon que d'une part l'agent a déjà une expérience du télétravail ou non, d'autre part que l'agent a déjà une expérience des activités nouvelles ou non.

B. La décision d'autorisation

Le responsable notifie à l'agent qui a fait la demande la décision.
Le responsable transmet cette décision à la DRH.
Dans le cas où il y aurait un nombre de demandes très supérieur à l'enveloppe budgétaire définie pour le télétravail, la DRH alertera le président, qui priorisera les demandes.

- Si elle est favorable, elle doit préciser les fonctions exercées en télétravail, le lieu d'exercice du télétravail, le/les jour(s) de télétravail, la durée d'autorisation, les horaires de la / des journée(s) télétravaillée(s).
Le responsable remet également à l'agent la charte du télétravail à l'UCA.

- Si la décision est défavorable, l'agent peut saisir la CPE, qui statuera sur sa demande. L'avis de la CPE est transmis au président, qui tranche sur la question.

La demande de télétravail peut également émaner du Service de Santé au Travail. Dans ce cas, après entretien avec l'agent, le SST transmet la demande d'autorisation à la DRH. La DRH notifie l'autorisation de télétravail à l'agent, ainsi qu'au n+1 de l'agent concerné. L'autorisation précise les

fonctions exercées en télétravail, le lieu d'exercice du télétravail, le/les jour(s) de télétravail, la durée d'autorisation, les horaires de la / des journée(s) télétravaillée(s).
Sans préjudice des dispositifs particuliers existant en faveur des personnes en situation de handicap, à la demande des agents dont l'état de santé le justifie et après avis du médecin de prévention, il peut être dérogé pour six mois à la durée fixée en termes de jours télétravaillés. Le nombre de jours télétravaillés peut, dans ce cas, aller jusqu'à 5 jours par semaine.
Cette dérogation est renouvelable une fois après avis du médecin de prévention.

C. La durée de l'autorisation

La durée de l'autorisation du télétravail est d'un an maximum.
L'autorisation peut être renouvelée par le n+1, après validation par le directeur de la structure (responsable administratif, directeur d'unité, directeur de service central), et après entretien entre l'agent et le n+1.

Le caractère réversible du télétravail est un principe important dans la réussite de sa mise en œuvre. Aussi, par simple déclaration écrite au n+1 avec copie à la DRH, l'agent peut mettre fin au télétravail, sans délai de préavis.

Afin de permettre aux agents et aux responsables de s'assurer que le télétravail correspond à leurs attentes, il est préconisé que les autorisations accordées comprennent une période dite « d'adaptation » : au bout de trois mois, un point d'étape est réalisé au cours d'un entretien entre l'agent et son n+1. Au terme de ce bilan, le télétravail peut être poursuivi, ou bien réaménagé, ou bien suspendu. En cas de désaccord entre l'agent et son n+1, l'agent peut saisir la CPE, qui proposera un avis au président.

III. Les moyens mis à disposition par l'UCA

L'UCA met à disposition des agents en télétravail un ordinateur portable.
Le matériel mis à disposition de l'agent à son domicile est la propriété de l'UCA et reste à usage professionnel. L'agent prend soin du matériel mis à sa disposition. En cas de dysfonctionnement de ce dernier, l'agent avertit immédiatement l'assistance informatique qui assure la maintenance.
Toutefois le support informatique de l'UCA ne couvre pas l'absence momentanée ou durable de connexion internet depuis le lieu de télétravail. Il est de la responsabilité du télétravailleur de signaler et de résoudre ce problème de connexion en s'adressant à son fournisseur internet et de le signaler à son supérieur hiérarchique (et non au support informatique).
Les appels téléphoniques professionnels sont transférés vers le téléphone personnel de l'agent pendant les plages horaires de télétravail, dans le cas où il n'est pas équipé d'un téléphone portable professionnel ou d'un dispositif équivalent.
Lorsque cesse le télétravail, l'équipement mis à disposition de l'agent dans le cadre du télétravail est restitué à l'UCA.
L'annexe 2 précise les éléments techniques.

IV. Les droits et obligations de l'agent en télétravail

A. L'environnement de travail au domicile

L'agent en télétravail doit prévoir un espace de travail permettant l'usage d'équipements destinés aux échanges téléphoniques ou vidéo ainsi qu'à la transmission et à la réception de données numériques compatibles avec l'activité professionnelle.

Pour la mise en oeuvre du dispositif, le lieu de télétravail est une adresse pour laquelle l'agent devra produire une attestation multirisques habitation permettant l'exercice du télétravail ainsi qu'un certificat ou à défaut une attestation sur l'honneur de conformité électrique. Les prises électriques utilisées dans l'espace de télétravail doivent être protégées par un disjoncteur différentiel 30mA. Dans ce cadre, l'UCA fournit à l'agent un descriptif de la conformité attendue des installations au domicile de l'agent.
En cas d'absence de certificat ou à défaut d'attestation sur l'honneur de la conformité électrique et d'attestation d'assurance habitation couvrant les activités de télétravail, la mise en place du télétravail ne peut être autorisée.
Il est recommandé à l'agent de réserver un « espace télétravail » à son domicile avec une surface minimale dotée d'un mobilier adapté, correctement éclairé et isolé des bruits extérieurs et intérieurs.

B. La protection des données par l'agent

Les règles relatives à la sécurité des systèmes d'information et de protection des données pour les agents en fonctions sur site s'appliquent aux agents en télétravail. L'agent en télétravail doit veiller à l'intégrité et à la bonne conservation des données auxquelles il a accès dans le cadre professionnel. Il s'engage à respecter la confidentialité et protéger l'intégrité des informations détenues ou recueillies dans le cadre de son activité et à veiller à ce qu'elles ne soient pas accessibles à des tiers. Les dispositions relatives à l'usage des technologies de l'information et des communications en vigueur (la charte générale à l'usage des ressources numériques de l'UCA, en annexe 3) au sein du service s'appliquent à l'agent en télétravail.

C. Le temps de travail

La réglementation relative au temps de travail, telle que définie par la délibération de CA n°CCCCC (annexe 4) s'applique aux agents en télétravail.

D. La santé et la sécurité sur le lieu de télétravail

Les dispositions législatives et réglementaires en matière de santé et de sécurité au travail s'appliquent à l'agent en télétravail.
Notamment, les risques inhérents aux situations de télétravail doivent être transcrits dans le document unique d'évaluation des risques professionnels (DUERP), ainsi que les actions de préventions associées. Ils doivent faire l'objet d'une mise à jour au minimum annuelle.
Ainsi, tout accident survenu sur le lieu d'exercice du télétravail pendant la plage horaire de télétravail et dans l'exercice de son activité professionnelle est soumis au même régime que s'il était survenu dans les locaux de l'établissement ou du lieu d'affectation.
Conformément aux compétences accordées au comité d'hygiène, de sécurité et des conditions de travail (CHSCT) par l'article 52 du décret n° 82-453 du 28 mai 1982 modifié relatif à l'hygiène et à la sécurité du travail ainsi qu'à la prévention médicale dans la fonction publique, les membres du CHSCT peuvent réaliser des visites sur le lieu d'exercice des fonctions en télétravail.
Dans le cas où l'agent exerce ses fonctions en télétravail à son domicile, l'accès à son domicile est subordonné à son accord formulé par écrit et transmis à la DRH. L'agent doit avoir été informé dix jours à l'avance au minimum.
En cas d'indisponibilité pour cause de maladie ou d'accident du travail un jour télétravaillé, l'agent est tenu aux mêmes obligations de transmission des justificatifs requis que celles auxquelles sont soumis les agents travaillant sur site.

V. Télétravail occasionnel

De façon occasionnelle, un agent peut demander de réaliser une mission en télétravail. C'est le n+1 qui instruit cette demande et donne son accord, et transmet l'information à la DRH (formulaire en annexe 1).

Cette demande ne peut être satisfaite que sous réserve d'un matériel informatique UCA disponible.

Ce télétravail occasionnel est limité à 10 jours par an.

Les télétravailleurs occasionnels ont les mêmes obligations de sécurité que les télétravailleurs réguliers.

UNIVERSITÉ Clermont Auvergne

Formulaire de demande de télétravail

Personnels de Bibliothèques, Ingénieurs, Administratifs, Techniques, Sociaux et de Santé

ETAPE 1 : à renseigner par l'agent - demande transmise par voie hiérarchique au directeur de service ou de composante

AGENT			
Nom et prénom :			
Composante/service :			
Poste occupé :			
Date d'arrivée sur le poste :		**Quotité de travail :**	
Statut :	☐titulaire (non stagiaire) ☐CDI	**Corps/grade/équivalent :**	

DETAIL DE LA DEMANDE

- Nature de la demande :

  ☐ première demande ☐ renouvellement

  télétravail régulier Télétravail occasionnel (10 jours par an maxi)

  Mon temps de trajet Aller ou Retour est de (joindre justificatif Mappy …) :

  ☐ Je bénéficie d'un aménagement de poste préconisé par le Médecin du travail (joindre le justificatif)

  ☐ Je travaille en Zone à Régime Restrictif- ZRR (joindre l'avis du fonctionnaire de sécurité et de défense)

Je demande à télétravailler à compter du :	Jusqu'au :				
Jour(s) hebdomadaires de télétravail : (les lundis et vendredis sont incompatibles)	☐lundi	☐mardi	☐mercredi	☐jeudi	☐vendredi

Motif de la demande et activités proposées en télétravail :

- Je dispose d'une connexion internet haut débit à mon domicile (lieu du télétravail) : ☐ OUI ☐ NON
- Je dispose d'un ordinateur portable professionnel : ☐ OUI ☐ NON
- Je dispose d'un téléphone portable professionnel : ☐ OUI ☐ NON

L'agent déclare avoir pris connaissance de la charte télétravail et de la charte informatique de sécurité des systèmes d'information :

date et signature de l'agent à l'origine de la demande

ETAPE 2 : à renseigner par l'encadrant ainsi que par le directeur de service/composante

ENTRETIEN ENTRE L'AGENT ET L'ENCADRANT	
Date de l'entretien :	
Avis de l'encadrant sur la demande de télétravail de l'agent : Détermination du besoin d'équipement à voir avec la DSI (Gilles RECH ou David ROMEUF)	☐ **FAVORABLE** ☐ **DEFAVORABLE**

• **SI AVIS FAVORABLE DE L'ENCADRANT, MODALITES DE TRAVAIL VALIDEES LORS DE L'ENTRETIEN :**					
télétravail à compter du :	Jusqu'au :				
Jour(s) hebdomadaires de télétravail: (les lundis et vendredis sont incompatibles)	☐lundi	☐mardi	☐mercredi	☐jeudi	☐vendredi
Aménagements spécifiques éventuels- (pics d'activité)					

Motivations par l'encadrant de l'avis favorable (précision des activités télétravaillées)

Précision des outils de suivi

• **SI AVIS DEFAVORABLE DE L'ENCADRANT, MOTIVATIONS DU REFUS :**

Nom, prénom et signature de l'encadrant : date :

Avis du directeur de service ou composante

Nom, prénom et signature du directeur : date :

VOTRE DOSSIER DOIT COMPORTER LES PIECES SUIVANTES

La présente demande de l'agent complétée de l'avis de l'encadrant et du directeur (ETAPES 1 et 2), est transmise par la voie hiérarchique à la DRH accompagnée des documents complémentaires ci-dessous utiles à l'analyse de la demande :

- **Annexe :** la description du domicile en vue du télétravail,
- **Annexe** : attestation de conformité du système électrique,
- **Annexe** : Evaluation des risques liés aux activités de télétravail,
- Attestation d'assurance multirisques **télétravail** habitation couvrant la période
- Fiche de poste,

Le cas échéant, justificatif du temps de trajet (Mappy, le trajet le plus court), aménagement préconisé par le médecin du travail, avis du fonctionnaire sécurité défense.

Les **annexes 1, et 5.1** sont des documents préparatoires à l'entretien entre l'agent et son responsable : ils n'ont pas vocation à être retournés à la DRH.

ANNEXE 1 - FICHE « AUTO-EVALUATION DE L'AGENT »

Document préparatoire à l'entretien entre l'agent et son responsable

(cette annexe n'est pas à retourner à la DRH)

MES MISSIONS			
	OUI	NON	NSP
Mes responsabilités et mes missions me permettent d'effectuer une partie de mes activités en dehors de mon site de travail	☐	☐	☐
Ma présence physique quotidienne sur site n'est pas indispensable à la réalisation de mes missions	☐	☐	☐
Mes réunions et contacts professionnels indispensables peuvent se gérer par des moyens de communication à distance ou peuvent être concentrés sur mes journées de travail sur site	☐	☐	☐
Je travaille en Zone à Régime Restrictif (joindre avis fonctionnaire sécurité défense)	☐	☐	☐
MES MOTIVATIONS POUR LE TELETRAVAIL			
	OUI	NON	NSP
Je bénéficie d'un aménagement de poste préconisé par le médecin du travail (joindre le document correspondant à la demande)	☐	☐	☐
Mon temps de trajet domicile-travail (aller ou retour) est d'une durée supérieure à 45 minutes et s'effectue dans des conditions parfois difficiles (retard, afflux voyageurs…)	☐	☐	☐
Je souhaite mieux concilier mes temps de vie personnelle et professionnelle	☐	☐	☐
Je souhaite bénéficier de plus d'autonomie dans l'organisation de ma journée de travail	☐	☐	☐
Une partie de mes missions demande une concentration qui sera favorisée par un environnement de travail isolé	☐	☐	☐
MON STYLE DE TRAVAIL ET MON APTITUDE AU TELETRAVAIL			
	OUI	NON	NSP
Je sais travailler seul(e) chez moi de manière aussi efficace que sur mon site de travail	☐	☐	☐
Je suis autonome et sais prendre des initiatives	☐	☐	☐
Je suis disponible et réactif	☐	☐	☐
Je respecte les délais qui me sont demandés	☐	☐	☐
Je suis organisé(e), je sais planifier et hiérarchiser mes tâches	☐	☐	☐
Je suis conscient(e) que mon organisation entre jours travaillés et jours télétravaillés pourrait être modifiée en fonction des impératifs supérieurs du service, sans récupération possible, et je suis capable de m'y adapter facilement	☐	☐	☐
Je ne crains pas l'isolement, en travaillant seul(e) chez moi	☐	☐	☐
MON STYLE DE TRAVAIL ET MON APTITUDE AU TELETRAVAIL			
	OUI	NON	NSP
Je pense être capable de maintenir de bonnes relations professionnelles avec mes collègues et mon supérieur même en situation de télétravail	☐	☐	☐
Je suis capable d'effectuer efficacement mes tâches même avec un suivi direct limité de mon supérieur hiérarchique	☐	☐	☐
Je suis à même de m'imposer des périodes de travail à domicile et de les respecter	☐	☐	☐
Je rends régulièrement compte de l'avancement de mon travail à mon supérieur hiérarchique	☐	☐	☐
J'arrive à gérer mon temps de travail de manière à fixer une frontière entre vie personnelle et vie professionnelle	☐	☐	☐
Je maîtrise les logiciels informatiques les plus couramment utilisés (bureautique, internet, messagerie…)	☐	☐	☐

MON ESPACE DE TELETRAVAIL			
	OUI	NON	NSP
Je dispose d'un espace dédié au télétravail, au calme, isolé	☐	☐	☐
Cet espace est assez spacieux pour y installer mon équipement de travail	☐	☐	☐
Je dispose d'une connexion internet haut débit	☐	☐	☐
Mes installations électriques sont conformes aux normes exigées par mon employeur	☐	☐	☐
Je dispose d'un ameublement adapté au travail	☐	☐	☐
Mon domicile fait l'objet d'un contrat d'assurance multi risques habitation	☐	☐	☐
MA SITUATION PERSONNELLE			
	OUI	NON	NSP
Je ne risque pas de déranger quand je travaille chez moi	☐	☐	☐
Les membres de ma famille respectent mon environnement de télétravail et acceptent que je travaille à domicile	☐	☐	☐
Si j'ai des enfants en bas âge, je dispose d'un mode de garde me permettant de télétravailler en toute sérénité	☐	☐	☐
Dans mon foyer et à mon domicile, je suis seul(e) à exercer mon activité professionnelle dans le cadre du télétravail	☐	☐	☐

ANNEXE 2 - DESCRIPTION DU DOMICILE EN VUE DU TELETRAVAIL

A renseigner par l'agent candidat au télétravail

(Annexe à retourner à la DRH)

1-Précisez ci-dessous l'adresse de votre domicile (lieu du télétravail):

2-Décrivez ci-dessous succinctement votre domicile :

3 Votre installation électrique
a été mise en conformité en quelle année :
par qui ou par quelle entreprise :
A partir de la prise murale, utilisez-vous une ou plusieurs multiprises : ☐OUI ☐NON Si oui quel type de multiprises (avec interrupteur ou autre protection) : Si plusieurs multiprises, sont-elles reliées les unes aux autres : ☐OUI ☐NON

4- Décrivez brièvement la pièce où s'effectue le télétravail :
Dimensions du plan de travail, type de siège, mobilier et équipements présents Merci de vérifier que votre lieu de travail est adapté ….. Rappel (texte élaboré par l'ergonome) L''agent s'engage à mettre en œuvre ces recommandations.

Date : Signature de l'agent

ANNEXE 3 – CONFORMITE ELECTRIQUE ATTESTATION SUR L'HONNEUR

A renseigner par l'agent candidat au télétravail

(Annexe à retourner à la DRH)

Je soussigné(e), atteste sur l'honneur qu'à ce jour le système électrique de mon domicile situé :

dispose d'un disjoncteur situé à l'intérieur de l'habitation et facilement accessible

- est protégé par un tableau électrique qui distribue et contrôle les différents circuits électriques alimentant chaque pièce de l'habitation et spécifiquement la pièce où je télétravaille
- est relié à la terre
- est conforme à la règlementation française en vigueur et me permet d'exercer mon activité professionnelle dans toutes les conditions de sécurité relatives aux systèmes électriques telles que prévues par les dispositions législatives et règlementaires en vigueur en France.

Date :

Signature de l'agent

ANNEXE 4.1 – Evaluation des risques liés aux activités de télétravail
Note explicative

Lors du télétravail l'agent est également exposé à des risques professionnels. Comme pour les situations de travail courantes, ces risques doivent être identifiés ainsi que les mesures de prévention permettant de les maitriser.
La démarche d'évaluation des risques est de la responsabilité du chef de service. Pour le télétravail cette évaluation est conjointe entre le chef de service et le futur télétravailleur car le lieu de travail est le domicile du télétravailleur.
Vous trouverez ci-dessous les principaux risques identifiés et une liste non exhaustive des mesures de prévention que vous pouvez mettre en place.

Risques	Exemples de mesures de prévention
Risques Psychosociaux : - Isolement social et professionnel - Difficulté à scinder vie privée / vie professionnelle - Management du télétravailleur - Désocialisation causée par la distance - Rejet des collègues - Passage au télétravail	-Réunion de service hors période de télétravail. -Réunion bilan au retour du télétravail -Respect par manager et télétravailleur des horaires de télétravail définis -Point téléphonique dans la journée -Questionnaire auto évaluation sur aptitude au télétravail permettant une prise de conscience sur les problématiques du télétravail (annexe 1) -Formation pour manager de télétravailleurs, -Formation pour futur télétravailleurs -Possibilité arrêt du télétravail par une des deux parties à tout moment par écrit
Risque du travailleur isolé	-Fourniture d'un téléphone portable -Contact téléphonique ou mail dans la journée -Présence d'une tierce personne
Risque travail sur écran	-Pauses régulières -Ergonomie du poste de travail (voir annexe 2)
Risque électrique	-Conformité électrique (voir annexe 4)
Risque de chute de plain-pied	-Dégagement des surfaces encombrées -Pièce dédiée au télétravail -Rampe en cas d'escalier

ANNEXE 4.2 – Evaluation des risques liés aux activités de télétravail
A renseigner conjointement par le chef de service et l'agent candidat au télétravail
(Annexe à retourner à la DRH)

Risques	Mesures de prévention
Risques Psychosociaux : - Isolement social et professionnel - Difficulté à scinder vie privée / vie professionnelle - Management du télétravailleur - Désocialisation causée par la distance - Rejet des collègues - Passage au télétravail	
Risque du travailleur isolé	
Risque travail sur écran	
Risque électrique	
Risque de chute de plain-pied	

Signature, date et tampon du chef de service

Mise en place du télétravail à l'UCA
Montée en puissance du dispositif

L'UCA a décidé de mettre en place le télétravail.
Ce mode d'organisation du travail, prévu pour les agents BIATSS, permet de mieux prendre en compte l'articulation entre la vie personnelle et la vie professionnelle, la qualité du travail, et la préservation de l'environnement. C'est aussi un facteur important de la santé au travail.

La Direction Opérationnelle des Systèmes d'Information a établi les conditions techniques de mise en oeuvre du télétravail et estimé les coûts financiers à supporter.
Le coût d'investissement d'un portable équipé, plus deux stations/ écran 24" avec clavier et souris est estimé à 1830 € TTC.
Le coût d'exploitation ramené au poste pour la DOSI est estimé à 100 euros.
Soit un total par poste évalué à 1930 euros.

Il est proposé que la mise en place du télétravail (télétravail "régulier") se fasse par étapes sur une période de 3 ans .
S'agissant d'une nouvelle modalité pour l'UCA et réservée aux seuls agents volontaires, il est en effet prérérable de prévoir une montée en puissance progressive. Une évaluation régulière du déploiement du dispositif permettra les éventuelles adaptations nécessaires tant sur le plan technique que sur le plan des usages du télétravail.
Il est proposé à ce sujet, que le groupe de travail constitué pour préparer la mise en place du télétravail soit également en charge du suivi de sa mise en oeuvre, pendant les 3 années de lancement du dispositif. Le groupe de travail présente le bilan annuel du télétravail en CHSCT et CT.

Sur la base d'un coût unitaire d'investissement de 1930 € par poste , il est proposé de choisir une trajectoire qui permette d'atteindre une cible de 100 télétravailleurs d'ici 3 ans :
Année 1 : 50 télétravailleurs pour un coût de 96 500 €
Année 2 : 25 télétravailleurs supplémentaires pour un coût de 48 250 €
Année 3 : 25 télétravailleurs supplémentaires pour un coût de 48 250 €

Cette trajectoire de déploiement peut être considérée en l'état actuel du dossier comme une trajectoire moyenne. En fonction de l'évaluation qui sera faite chaque année, des réajustements pourront être envisagés à la hausse avec une montée en puissance en 2 ans au lieu de 3 (en gardant une cible de 100 télétravailleurs au terme de la période) ou à la baisse avec une montée en puissance plus lente si cela s'avère plus pertinent.

En tout état de cause, le maintien d'un objectif de 100 télétravailleurs permet d'arrêter d'ores et déjà une estimation financière du coût de l'ensemble de l'opération.

Il est également propose une montée en puissance progressive quant à la sécurisation des données. La première année, certains logiciels et applications spécifiques ne seront pas autorisés en télétravail du fait du caractère critique des données manipulées (ex : les application du SI métier – RH, finances,…). Au terme de la première année, un bilan sera établi, et en fonction du nombre de demandes non satisfaites et des possibilités financières de l'établissement, il pourra être décidé d'ouvrir le télétravail aux missions réalisées sur des logiciels et applications spécifiques.

Le télétravail à l'UCA

Préconisations et accompagnement
par la DOSI
Direction Opérationnelle des Systèmes d'Information

Document de travail

UNIVERSITÉ Clermont Auvergne

Mise en œuvre

1. Usages et Outils.
2. Prérequis et préconisations techniques.
3. Support informatique.
4. Coûts financiers estimatifs du poste du télétravailleur.

1. Usages et outils

La mission du télétravailleur s'effectue dans un cadre maitrisé et précis:

- Ce cadre de travail doit être validé par le CA de l'UCA.
- Certains logiciels ou applications spécifiques peuvent ne pas être autorisés en télétravail du fait de l'incomplétude de leur niveau de sécurisation ou du caractère critique des données manipulées (par exemple les applications du SI métier – RH, finances, ….
- L'accomplissement de travaux nécessitant l'accès à des données d'une volumétrie importante, à des données à caractère sensible au sens du RGPD ou de la protection du patrimoine scientifique, globalement à des données dont la divulgation, l'altération ou la manipulation aurait des conséquences sur l'accomplissement des missions de l'établissement sont proscrits en télétravail.
- Un point est fait en amont avec le responsable hiérarchique sur les documents de travail autorisés.

UNIVERSITÉ Clermont Auvergne

1. Usages et outils

Le télétravailleur bénéficie de plusieurs outils:

- La messagerie électronique : l'outil supporté par la DOSI est le webmail zimbra
- Le stockage centralisé des données: les données manipulées dans le cadre du télétravail sont accédées exclusivement à partir de la plateforme UcaDrive. Le transfert et l'usage des données via des supports « papier » ou amovibles (clés usb, disques) est vivement déconseillé.
- Le panel d'outils offerts sur https://ent.uca.fr (prise de rendez-vous, messagerie instantanée, réservation de salles ou de matériel, gestion de groupes, …) et les outils en ligne RENATER (webconférence, …)
- Un outil logiciel de téléphonie sur Internet de type « softphone » - disponibilité fin 2019

2. Prérequis et préconisations techniques

Sur le lieu de télétravail :

- Une connexion Internet de 20Mb/s minimum est mise en œuvre à la charge du télétravailleur (l'absence momentanée ou durable de connexion internet sur le lieu de télétravail est à signaler au responsable hiérarchique et non au support informatique).
- Le poste de télétravail est connecté par câble ethernet à la box.
- Les termes de la charte des usages du numérique de l'UCA sont respectés, en particulier les consignes de sécurisation des sessions de travail (authentification sur la machine avec le compte ENT, mot de passe fort, non session à un tiers de ses identifiants de connexion, verrouillage/fermeture de la session de travail en cas d'absence même de courte durée, pas d'enregistrement des mots de passe dans les navigateurs, ….).
- L'usage de documents dématérialisés est privilégié, pas d'impression en local.

UNIVERSITÉ Clermont Auvergne

2. Prérequis et préconisations techniques

Sur l'équipement informatique du télétravailleur :

- Il s'agit d'un équipement mobile impérativement fourni par l'établissement. L'attribution se fait à titre permanent ou dans le cas d'un dispositif de prêt pour un télétravail occasionnel. Dans ce dernier cas le télétravailleur veillera à travailler sur ses documents depuis la plateforme UcaDrive et l'équipe informatique nettoie la machine entre deux prêts.

- Le disque dur de l'équipement doit être chiffré, quelque soit le système d'exploitation.

- L'équipement fourni est un outil de travail. Son accès est autorisé au seul télétravailleur. Comme sur le lieu d'affectation, son usage à titre privé est toléré dans le respects des termes de la charte des usages du numérique.

- Le télétravailleur reste vigilant sur les modalités de stockage de l'équipement en dehors du lieu d'affectation pour garantir sa sécurité et sa pérennité.

2. Prérequis et préconisations techniques

Sur l'accès distant au réseau de l'établissement :

- Aucun équipement personnel ne doit être utilisé dans le cadre d'un accès distant au réseau interne de l'entreprise (hors réseau éduroam ou éduspot)

- La connexion doit être chiffrée, authentifiée et journalisée conformément à la réglementation et à la Politique de Sécurité des Système d'Information – PSSI - de l'UCA. Cela signifie que l'équipe informatique en charge de la gestion de l'accès distant s'appuie sur une infrastructure disposant d'un parefeu paramétré et administré conformément à cette politique de sécurité et permettant des connexions de type VPN.

- Toute demande d'accès distant doit faire l'objet du remplissage du formulaire prévu à cet effet. Ce formulaire est renseigné par le télétravailleur et son responsable hiérarchique ainsi que le responsable informatique de la structure. Il est disponible auprès des équipes informatiques de la DOSI.

3. Support informatique de la DOSI

Le support informatique par la DOSI:

- est assuré exclusivement à partir de l'ouverture d'un ticket sur support.dsi@uca.fr
- est assuré exclusivement sur du matériel et des applications professionnels, inventoriés et administrés par les équipes informatiques.
- peut faire l'objet d'une prise en main à distance que le télétravailleur autorisera à destination des agents de la DOSI avec des outils qualifiés par cette dernière.
- ne couvre pas l'absence momentanée ou durable de connexion internet depuis le lieu de télétravail.

4. Coûts financiers estimatifs du poste du télétravailleur

Les coûts suivants sont calculés par rapport au cadre défini dans le présent document, à savoir sans accès aux applications du SI métier.

- tarifs fin déc. 2018
- portable seul = 1128€TTC
- portable + 1 station/écran 24"/clavier/souris = 1479TTC
- portable + 2 stations/écrans 24"/clavier/souris (ordi + station accueil/écran domicile + station accueil/ecran lieu de travail) = 1830€TTC
- softphone (licence + micro-casque) : ?

UNIVERSITÉ Clermont Auvergne

CHARTE GENERALE A L'USAGE DES RESSOURCES NUMERIQUES

Université Clermont Auvergne

Table des matières

1. Contexte et définitions

1.1 Introduction

L'usage de ressources numériques est devenu systématique, commun et indispensable au déroulement des missions des universités et de leurs usagers. Les ressources numériques sont également devenues l'objet de nombreuses convoitises et de détournement à des buts malveillants, constituant autant d'actes illégaux ou indésirables pour l'établissement.

Le présent document nommé « Charte générale pour l'usage des ressources numériques » a pour objet de décrire les conditions dans lesquelles les ressources numériques de l'Université Clermont Auvergne peuvent être utilisées par l'ensemble des usagers, et de préciser la responsabilité des usagers et de l'établissement en accord avec la législation et la réglementation. Il définit les règles de bonne utilisation et participe à la prise de conscience des devoirs, des responsabilités et des sanctions. Il est en ce sens un outil de protection des usagers et de l'établissement.

Cette charte générale s'adresse à l'ensemble des usagers de l'Université Clermont Auvergne, elle est opposable à tous. Le non-respect de cette charte engage la responsabilité personnelle de l'utilisateur. Elle est annexée au règlement intérieur de l'établissement.

La présente charte générale a été présentée devant le comité technique puis au conseil d'administration qui en a validé les termes et s'est prononcé favorablement pour son application à l'ensemble des Usagers. Ainsi, son acceptation par tout Usager devient une condition préalable à l'Accès aux Ressources numériques de l'Etablissement.

1.2 Définitions

Dans la présente charte, les termes principaux, identifiés par une majuscule, répondent aux définitions et commentaires suivants :

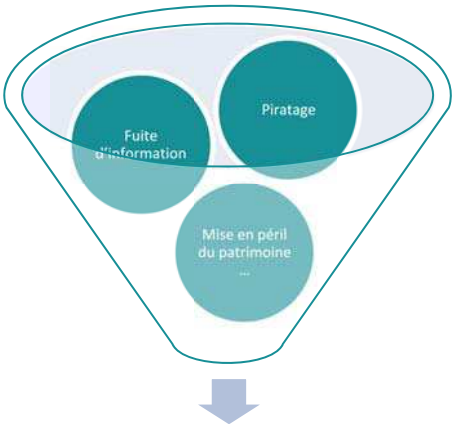
Terme utilisé	Définition	Commentaires
Etablissement	l'Université Clermont Auvergne	Prise en tant que personne morale disposant d'une capacité juridique
Administrateur	Agent ou prestataire chargé par la direction des systèmes d'information de l'Université Clermont Auvergne d'administrer et contrôler l'utilisation d'un système d'information ou de Ressources numériques de l'Université	
Usager	Apprenant (étudiant, stagiaire, …) ou autre personne physique (agent de l'UCA, intervenant extérieur) qui agissant pour son propre compte ou celui de son employeur utilise les ressources numériques de l'établissement dans le cadre d'une accréditation qu'il a reçu de l'Etablissement	Il s'agit des personnels permanents ou non et des intervenants hébergés, des étudiants, stagiaires et auditeurs, des partenaires, des fournisseurs et des invités qui interviennent temporairement dans un cadre contractuel défini.
Ressource(s) numérique(s)	Données numériques et tous moyens, composants, ou services numériques contribuant à accéder, collecter, stocker, transformer, diffuser ces données numériques	Qu'ils soient matériels ou logiciels, hébergés sur des serveurs internes ou externes exploités sous la responsabilité de l'Etablissement
Mission	Périmètre d'intervention légitime d'un Usager vis-à-vis de l'Etablissement	Il s'agit d'une mission professionnelle, d'une prestation, d'une inscription à un cursus d'apprentissage, de la participation à une conférence, de la fourniture de produits ou services, dont la finalité est établie, en fonction des usagers.
Accès ou accéder	Fait d'utiliser une Ressource numérique	L'Accès est entendu comme utilisation légitime, ayant nécessairement fait l'objet d'une Autorisation
Autorisation ou autoriser	Décision prise par l'Etablissement et conférant un caractère légitime à l'Accès à une Ressource numérique	-
Tiers	Désigne une personne physique ou morale différente de l'Etablissement	Le Tiers est qualifié de « conventionné » lorsqu'il a conclu avec l'Etablissement un accord autorisant ses Usagers à utiliser les Ressources numériques du Tiers
Charte(s) spécifique(s)	Chartes détaillées et dédiées à l'utilisation de ressources numériques à diffusion restreinte.	Ces chartes ne s'imposent qu'au cas par cas à des sous-ensembles restreints d'Usagers

1.3 Risques et opportunités

Les principes exprimés dans ce document sont applicables de façon générale et adaptés à la majorité des environnements.

Chaque Usager est invité à s'approprier le présent document, tant dans l'intérêt de sa mission auprès de l'Etablissement que dans son intérêt propre.

Afin d'utiliser les Ressources numériques de manière optimale, et de se prémunir contre les risques principaux.



Les risques relatifs aux Ressources numériques sont nombreux

1.4 Caractère opposable de la charte générale

L'utilisation des Ressources numériques mises à disposition par l'Etablissement implique un respect strict de la présente charte générale par chaque Usager. La charte générale présente un caractère opposable.

2. Usage des Ressources numériques

2.1 Définitions

Pour les besoins de l'accomplissement de leurs Missions, l'Université met à la disposition de ses Usagers des Ressources numériques présentées dans le tableau ci-dessous :

Ressources numériques

- **Infrastructure réseaux** : *à portée locale, nationale (Renater) et publique, que ces infrastructures soient filaires ou non filaires*
- **Données collectées et produites** *: que ce soit dans le domaine administratif, pédagogique, documentaire ou de la recherche*
- **Matériels informatiques :** *ordinateurs fixes et portables, serveurs, tablettes, ordiphones et sous-jacents : serveurs, switchs, firewall*
- **Applications :** *portails internet, extranet, intranet, logiciels et progiciels de gestion, logiciels et progiciels spécialisés, logiciels et progiciels bureautiques et utilitaires, messagerie*
- **Support d'identification et d'authentification :** *badges étudiants et personnels RFID, cartes magnétiques, certificats de signature numérique*
- **Espaces de stockage :** *internes, externes et mobiles*
- **Matériels techniques accédant aux ressources :** *téléphonie fixe et mobile, moyens de reprographie, périphériques connectés, fax*
- **Tout produit ou service numérique :** *dès lors que pour être utilisé il nécessite le recours à l'un ou l'autre des produits ou services mentionnés ci-dessus*
- **….**

A noter : Tout accès à des moyens ou services numériques tiers depuis un matériel ou des réseaux de l'Etablissement, implique de fait l'accès à des ressources numériques de l'établissement.

2.2 Autorisation et protection de l'Accès aux Ressources numériques

L'Accès à chacune des ressources numériques est soumis à Autorisation. Une Autorisation s'obtient soit automatiquement en fonction de profils d'Usagers, soit sur demande par voie hiérarchique, ou encore lorsque ne sont pas établis de liens hiérarchiques, par une demande auprès du représentant administratif d'une entité dans laquelle s'opère la Mission.

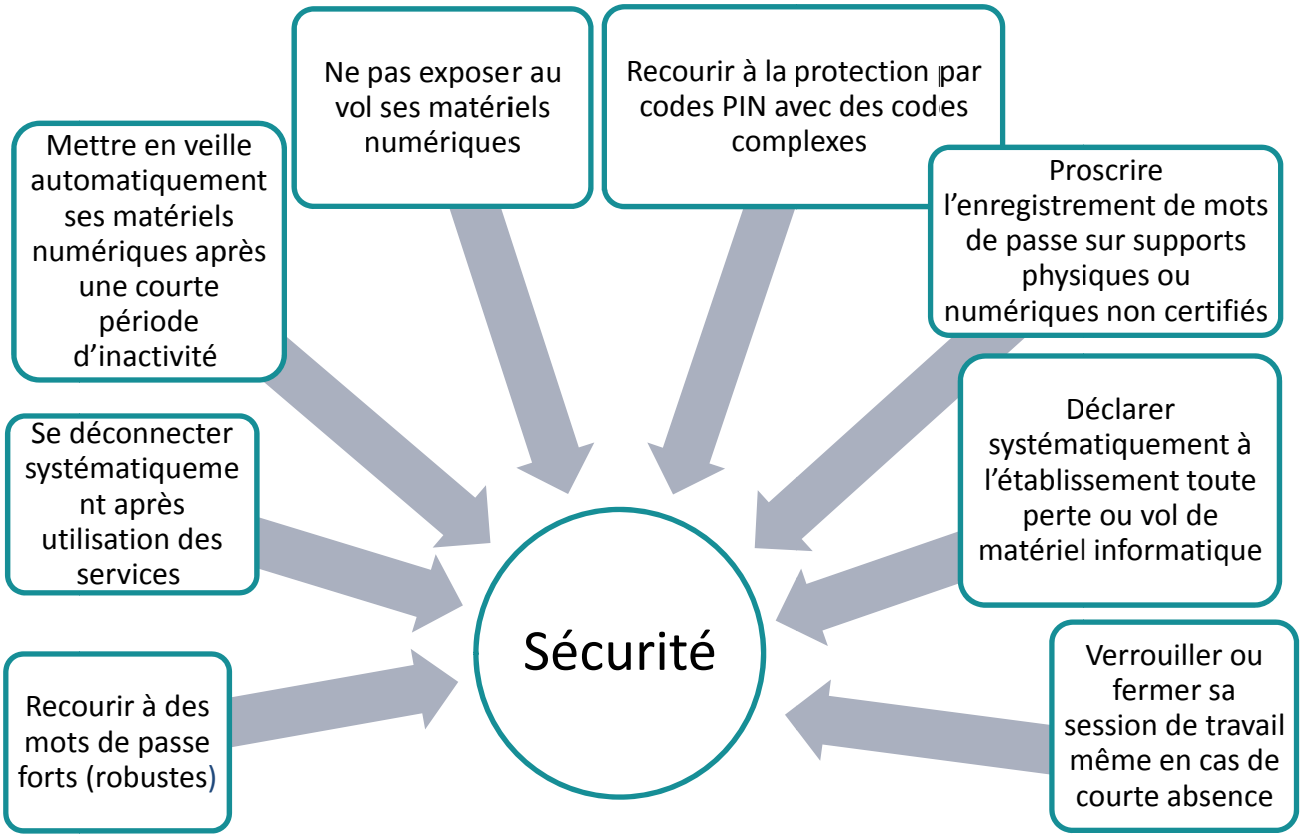
Cette Autorisation est confiée à titre personnel par l'Administrateur à chaque Usager et pour une durée déterminée correspondant le plus souvent à la durée de sa Mission.

L'Autorisation s'accompagne de la délivrance à l'Usager par l'Administrateur d'un identifiant et d'un mot de passe confidentiel et strictement personnel. Ces moyens d'authentification sur le réseau informatique et plus généralement vis-à-vis des Ressources numériques de l'Etablissement ne doivent être en aucun cas ni communiqués ni cédés à un Tiers.

Il appartient à chaque Usager de prendre les précautions nécessaires pour protéger ses identifiants, afin que ceux-ci ne soient pas divulgués à des Tiers. Le compte informatique en particulier est strictement personnel et incessible. Il en est de même pour tout moyen d'identification/authentification physique ou numérique (par exemple certificat de signature électronique).

A savoir : Chaque Usager est responsable de l'utilisation qu'il fait des Ressources numériques via les Autorisations d'accès qui lui ont été confiées.

Pour se protéger, l'Etablissement recommande à ses Usagers les mesures suivantes :



Liste non exhaustive donnée à titre indicatif

A ces fins, l'usager qui en fait la demande (contacts disponibles dans les « mentions légales » du site web de l'université), peut prendre connaissance des documents de référence, internes ou externes. Ils déclinent les bonnes pratiques en matière de protection d'Accès en cas de menace potentielle ou avérée du patrimoine informationnel de l'Etablissement.

L'Usager ne peut s'opposer au droit de l'Etablissement d'accéder à toutes Ressources numériques, y compris les ressources matérielles qui lui auront été prêtées. Les interventions menées par les équipes techniques, sous la direction et le contrôle de l'Administrateur se déroulent de deux manières :

- **Intervention à distance** : l'équipe technique prend le contrôle du matériel avec l'accord préalable de l'Usager.

- **Intervention physique** : lorsque nécessaire, l'équipe technique fixe un rendez-vous à l'Usager qui s'engage à rendre disponible le matériel requis. Il peut obtenir un matériel de prêt sous réserve de disponibilité.

A savoir : un administrateur de systèmes ne demandera jamais à un usager de lui communiquer son mot de passe (ni par courriel, ni de visu). Il pourra exceptionnellement l'inviter à se connecter à un système auquel il doit accéder au nom de l'Usager pour les besoins de sa Mission. Les mots de passe sont enregistrés dans les serveurs universitaires sous forme sécurisée, si bien qu'un administrateur lui-même ne peut les relire.

En cas d'absence de l'Usager (arrêt maladie, déplacement, congé, etc.) ou d'impossibilité pour l'Administrateur d'entrer en contact avec lui et s'il est fait obligation à l'Administrateur d'accéder aux données de l'Usager pour des motifs de sécurité ou d'exploitation, l'Etablissement se réserve la faculté de prendre toutes mesures nécessaires pour accéder aux données. Il est rappelé à cet égard que lorsqu'un accès aux données professionnelles est requis et en cas d'absence de l'agent dans une situation d'urgence risquant de conduire à un blocage ou un dysfonctionnement, la loyauté des relations entre l'Etablissement et l'agent autorise ce premier à accéder aux données de l'agent. Toute intervention dans ce sens se fera toutefois dans le respect de la vie privée conformément aux mesures prises préventivement par l'agent lui-même (cf paragraphe 2.4 de la présente charte, section « vie privée » à ce sujet).

2.3 Modification et suppression des Autorisations d'Accès

Toute Autorisation relative à l'usage des Ressources numériques prend fin naturellement lors de la cessation de la Mission auprès de l'Etablissement (fin de contrat ou d'année universitaire notamment). L'Autorisation peut être modifiée en fonction des évolutions de la Mission de l'Usager et/ou de la politique de l'établissement dans le sens d'une extension ou d'une restriction des droits d'Accès.

Un manquement au respect de la présente charte générale constitue un motif valable de modification, de suspension, voire de suppression d'une Autorisation.

A l'issue de la Mission de l'Usager, l'Etablissement est chargé de restituer les éventuelles données qui appartiendraient en propre à l'Usager et qui seraient conservées dans les Ressources numériques. L'Usager devra manifester son intention de les récupérer ou de les voir supprimer.

Les messages électroniques qui seraient adressés à l'Usager, après expiration de ses droits d'Accès aux Ressources numériques et suppression de ses données seront rejetés des systèmes de messagerie de l'Etablissement.

2.4 Droits relatifs aux données numériques produites dans l'exercice d'une mission professionnelle par un agent

Lorsqu'elles sont produites dans l'exercice d'une mission professionnelle, les données numériques sont de façon générale réputées être à caractère professionnel et appartenir dès lors à l'employeur. Certaines données dérogent néanmoins à ce cadre, lorsqu'elles relèvent de :

- la création d'œuvres de l'esprit pour laquelle l'agent n'a pas été explicitement missionné
- la vie privée, au titre du droit à la vie privée résiduelle qui peut s'exercer sur le lieu du travail dans les limites légales.

Œuvres de l'esprit

Le code de la propriété intellectuelle reconnaît aux auteurs de création d'œuvres de l'esprit un droit de titularité (également nommé droit d'auteur) qui s'exerce sous forme d'un droit moral inaliénable, et de droits patrimoniaux transférables et cessibles. L'employeur conserve le droit d'exploitation lorsqu'une œuvre de l'esprit a été créée dans le cadre de la mission professionnelle d'un agent et que l'agent a été missionné pour la réaliser. Une exception s'appliquant particulièrement au contexte universitaire concerne notamment les productions scientifiques et d'enseignement pour lesquels l'employeur peut ne pas bénéficier systématiquement de droit d'exploitation tacite dans la mesure où il n'oriente pas systématiquement la création des œuvres de l'esprit.

Vie privée

De même, l'intimité de la vie privée et le secret des correspondances électroniques privées sont garantis à l'Usager sauf dans les cas où la loi autorise leur limitation.

S'agissant des agents de l'établissement, un usage à titre personnel des ressources numériques professionnelles est toléré tant qu'il reste modéré et n'interfère pas avec leur mission professionnelle, et ce conformément au principe connu sous la dénomination de « vie privée résiduelle ». Cette tolérance d'usage porte autant sur les fichiers de données que sur les correspondances électroniques. Lorsqu'il s'agit de données personnelles ou de correspondances personnelles sous forme numérique, celles-ci doivent être identifiées explicitement comme telles sous la désignation de « privé et confidentiel » ; toute autre dénomination sera considérée comme non-opérante par l'Etablissement, conférant alors aux données un caractère professionnel. Pour autant, cette pratique n'exempte pas leurs détenteurs de se soumettre à la législation, notamment relative aux droits d'auteur des tiers et aux contenus illicites. L'ensemble des données privées et non-professionnelles restent accessibles dans le cadre d'une réquisition judiciaire.

A savoir : détenir illégalement des contenus protégés par les droits d'auteur (exemples : films, musiques, logiciels) sur un support professionnel engage à la fois la responsabilité de l'employeur pour contrefaçon et celle de la personne qui les a introduits. Ainsi accéder ou maintenir de tels contenus sur des espaces de stockage fournis par l'Etablissement constitue une faute.

Toutes autres données numériques manipulées dans le cadre d'une mission professionnelle sont réputées à caractère professionnel.

2.5 Accès illégitime aux données numériques professionnelles et personnelles

L'Etablissement déploie des moyens conséquents pour assurer la sécurité de ses Ressources numériques. Pour autant le niveau de sécurité est dépendant de nombreux facteurs. Certains dépendent directement de Tiers et dès lors ils ne peuvent être totalement maîtrisés par l'Etablissement, indépendamment des moyens déployés. Par ailleurs la volumétrie importante des systèmes sous-jacents est telle qu'elle ne permet pas à l'Etablissement de se prémunir totalement de tous types d'attaques malveillantes.

L'Accès aux données de toutes natures stockées sur les serveurs de l'Etablissement ne saurait constituer un Accès illégitime lorsqu'il est opéré par un administrateur technique dans le cadre strict de sa mission, ou par un prestataire placé sous sa responsabilité. La charte des administrateurs techniques protège les Usagers en ce sens, et définit les finalités pour lesquelles un administrateur technique intervient sur les données des Utilisateurs, et notamment : besoin de gestion (déplacement de fichier, sauvegarde, renouvellement de matériel), inspection extraordinaire sur incident ou alerte de sécurité informatique, réponse à une requête judiciaire. L'Etablissement est garant vis-à-vis des Usagers du strict respect de cette charte par les administrateurs techniques.

2.6 Le transfert de données par un Usager

Le transfert de données numériques est qualifié d'usage de Ressources numériques en ce qu'il utilise d'autres ressources numériques de l'Etablissement telles que le stockage ou les réseaux. Le transfert de données peut constituer une source de fuite ou de vol de données. Le transfert de données appartenant à l'Etablissement et opéré par un Usager lorsqu'il est agent, vers des tiers ou à destination d'un espace de stockage externe à l'Etablissement, ne peut s'effectuer que dans les termes d'une convention et sous le contrôle de l'Administrateur. Il doit être réalisé dans un cadre strict d'autorisation donnée par le représentant légal de l'Etablissement, que ce transfert relève directement ou non de la mission de l'agent.

En ce qui concerne la diffusion d'informations nominatives, elle n'est possible que dans le respect des prescriptions figurant à l'article 15 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Aucun Usager n'est a priori autorisé à procéder à un quelconque traitement (au sens de la loi « Informatique et Libertés ») de données à caractère directement ou indirectement personnel à l'aide des Ressources numériques, dès lors que ces données relèvent : des opinions politiques (y compris l'appartenance syndicale), philosophiques ou religieuses, de la préférence sexuelle, de la santé (élargie aux données génétiques et biométriques), des infractions pénales et condamnations, des appréciations relatives aux difficultés sociales, de l'identification NIR (numéro de sécurité sociale).

A savoir : envoyer des données sensibles dans un service de stockage « cloud » tels que DROPBOX, One Drive, GOOGLE Apps, GMAIL, et iCloud et ou service de traitement ou diffusion « cloud » tels que SKYPE, HANGOUT, ou ILovePDF non mis à disposition par l'Etablissement représente un risque élevé de fuites de données. Il convient de s'interroger sur la nature sensible des contenus numériques manipulés et de proscrire le recours à ce type de services dès lors que ceux-ci ne pourraient être diffusés publiquement sans risquer de compromettre l'Etablissement.

2.7 Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer la continuité de service en cas d'absence ou de départ, l'agent de l'établissement prendra toute disposition utile pour permettre l'accès à ses données professionnelles aux personnes habilitées. De son côté le responsable hiérarchique, informé, prendra les dispositions nécessaires pour garantir la conservation de ces informations.

A savoir : Vous pouvez demander la création d'une boite de messagerie fonctionnelle (par exemple directeur.dsi@uca.fr). Celle-ci sera ainsi consultable par plusieurs personnes en cas de votre abscence et permettra d'assurer plus facilement la continuité de service.

3. Devoir d'information

3.1 Devoir d'information auprès de l'Etablissement par les Usagers

Chaque Usager est tenu d'informer l'Etablissement, lorsqu'il constate qu'une Ressource numérique, qu'elle lui ait été confiée ou non, fait l'objet d'une compromission avérée, suspectée ou potentielle, de façon à évaluer les mesures à prendre pour limiter les impacts sur le SI. Exemples :

- intrusion par un tiers,
- diffusion ou détournement d'un compte ou mot de passe,
- usurpation d'identité,
- faits de négligence, conduite à risque,
- vol ou perte d'un moyen d'identification (badge) ou d'un matériel, y compris les matériels personnels dans le cas où ces matériels sont utilisés pour accéder à des ressources numériques de l'établissement,
- duplication, téléchargement, divulgation non-autorisés,
- acte de piratage, infection par un virus informatique, fonctionnement douteux d'une ressource numérique,
- atteinte au droit d'auteur.

De même, un Usager qui prendrait conscience d'avoir réalisé un acte contraire à la charte générale est invité à en informer l'Etablissement de façon à évaluer au plus tôt les mesures à prendre pour diminuer les impacts éventuels sur le Système d'Information.

3.2 Devoir d'information auprès des Usagers par l'Etablissement

L'Etablissement s'engage lorsqu'il en a connaissance à informer tout Usager dont les Ressources numériques ont fait l'objet d'un acte malveillant.

L'Etablissement est soumis à des obligations légales en ce qui concerne l'utilisation de ses Ressources numériques. Notamment, l'Etablissement est tenu d'enregistrer les accès aux Ressources numériques tierces via ses réseaux afin de s'assurer que ses propres Ressources informatiques ne soient pas utilisées à des fins illicites. Les données enregistrées peuvent être qualifiées de données à caractère personnel au sens de la loi du 6 janvier 1978 si les éléments enregistrés permettent d'identifier des personnes physiques.

Ces enregistrements sont conservés pour une durée d'un an. L'Etablissement peut être amené à produire ces logs de connexion dans le cadre d'une réquisition judiciaire. En aucun cas l'Etablissement n'accède à ces enregistrements pour ses besoins de gestion courants.

L'Etablissement se réserve la possibilité d'y accéder à titre exceptionnel lorsqu'il suspecte ou constate des cas de compromission et qu'il y va de la défense de ses intérêts propres ou de ceux de l'Usager. En dehors des cas susmentionnés, l'établissement s'interdit de consulter individuellement ces enregistrements et leur contenu.

Cette durée de conservation est limitative et ne peut excéder un an. De tels enregistrements existent également par défaut au sein de certaines applications logicielles et font partie intégrante des dispositifs de gestion et de sécurité mis en œuvre. Ces enregistrements peuvent être utilisés pour des besoins de gestion et d'administration : statistiques, débogage, protection contre la compromission, audit. En dehors de ces cas particuliers, l'Etablissement s'interdit de consulter individuellement ces enregistrements.

Enfin, la durée de conservation des données de travail à caractère personnel dans le système d'information se doit d'être compatible avec les missions de l'université et ses impératifs de gestion. Excepté pour les usagers de type intervenants invités qui entretiennent des relations à court terme avec l'établissement, les données à caractère personnel sont conservées dans les applications du système d'information tant qu'elles sont nécessaires à la gestion de leur dossier.

L'exploitation des données de travail à caractère personnel et des enregistrements se fait dans le respect de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Les usagers disposent d'un droit d'accès et de rectification qu'ils peuvent exercer auprès du CIL (Correspondant Informatique et Liberté) de l'établissement.

4. Surveillance du réseau et des Ressources informatiques

Pour assurer la meilleure sécurité informatique possible de l'Etablissement et une utilisation optimale des Ressources numériques par les Usagers, l'agent en charge de l'administration informatique est habilité à procéder à des vérifications régulières de la bonne utilisation de l'ensemble des postes et matériels informatiques, et plus généralement des Ressources numériques, confiés aux Usagers. Des statistiques d'utilisation pourront être établies et communiquées à la direction de l'Etablissement. A cet effet, l'Administrateur a mis en place des outils de surveillance de l'utilisation des Ressources numériques.

Toute mise en place de nouveaux outils de surveillance rendus nécessaires par l'évolution des besoins et des techniques sera précédée d'une information publiée sur l'intranet ou sur tout autre support en usage dans l'Etablissement. En outre, sur autorisation judicaire préalable, l'Administrateur a la possibilité d'ouvrir les boîtes aux lettres et tous les fichiers, y compris personnels.

Il peut également faire consigner tout ordinateur (PC ou portable) et tout matériel et ainsi interdire momentanément l'utilisation d'un matériel mis à la disposition d'un Usager, et de fait, interdire l'accès à internet et au serveur de messagerie électronique.

Aucune exploitation des informations dont l'Administrateur réseau peut avoir connaissance dans l'exercice de ses fonctions ne saurait être opérée sur son initiative ni sous ordre hiérarchique, à des fins autres que celles liées au bon fonctionnement et à la sécurité des Ressources numériques.

5. Droit à la déconnexion

Dans le respect des principes énoncés à l'article L. 2242-8 du code du travail, l'établissement met en œuvre tous les dispositifs de régulation nécessaires pour assurer le droit à la déconnexion du personnel. Par ailleurs, une charte spécifique à la messagerie électronique est élaborée pour garantir le bon usage de cet outil.

6. Chartes spécifiques

Des chartes spécifiques à certaines ressources complètent la présente charte générale. Ces chartes spécifiques concernent des ressources à diffusion restreinte et ne s'adressent qu'aux utilisateurs habilités à utiliser ou accéder à ces ressources. Les Ressources numériques de l'Etablissement évoluant en permanence de même que les dispositions légales et réglementaires, en voici ci-dessous une liste non exhaustive :

Les Chartes

- Charte de messagerie
- Charte nomade
- Charte des Administrateurs techniques
- Charte d'hébergement
- ....

L'accès à des ressources à diffusion restreinte par un utilisateur habilité de l'Etablissement implique l'adhésion aux chartes spécifiques en vigueur. L'acceptation de la présente charte générale vaut acceptation de ce principe. Selon la criticité des Ressources numériques mises en jeu, l'Etablissement pourra recueillir une acceptation explicite en sus.

7. Exemples de pratiques contrevenant à la charte générale

L'utilisation des Ressources numériques mises à la disposition des Usagers par l'Etablissement est réputée loyale et rationnelle. Sans viser l'exhaustivité, ce chapitre illustre quelques situations propres au contexte universitaire qui contreviennent à la présente charte et en présence desquelles l'Etablissement ou toute autorité hiérarchique compétente peut prononcer des sanctions.

Sur le respect de la propriété intellectuelle et du droit d'auteur, et de la protection des données réputées confidentielles :

- Télécharger, détenir, utiliser ou diffuser des contenus média (musiques, films, livres) licenciés sans en avoir acquitté les droits ;
- Reproduire, diffuser des cours, des podcasts, des éléments pédagogiques sur des portails publics sans accord de leur auteur ;
- Télécharger, détenir, utiliser ou diffuser des logiciels licenciés sans en avoir acquitté les droits ;
- Divulguer ou s'exposer à la fuite de secrets de fabrique ou d'informations couvertes par le secret des affaires ;
- Divulguer, stocker ou transférer des données à caractère confidentiel sur des systèmes tiers tels que Dropbox, Gmail, Skype, etc.

Sur le respect mutuel des personnes : un Usager ne doit ni porter atteinte à la vie privée et à la personnalité de quiconque, ni nuire à l'activité professionnelle d'un Tiers par l'utilisation des Ressources numériques :

- Tenir des propos injurieux, racistes, menaçants, diffamatoires, harcelants, obscènes, pornographiques, sectaires, portant atteinte à l'intégrité morale ou à la dignité humaine, et plus généralement illégaux ;
- Usurper l'identité d'autrui, même sans dessein de lui nuire, ou utiliser intentionnellement le compte d'un autre Usager.

Sur le respect de l'intégrité des Ressources numériques : aucune atteinte aux dispositifs de protection ne doit être portée par l'Usager, aucune recherche sur la sécurité des systèmes d'information ne peut être effectuée sans autorisation préalable et l'information du RSSI (Responsable de la Sécurité des Systèmes d'Information):

- Altérer les dispositifs de sécurité déployés : désinstallation des logiciels antivirus, modification des paramétrages des mises à jour logicielles, entraver le déroulement des procédures automatisées, non-respect des consignes données par les administrateurs techniques ;
- Effectuer des tentatives répétées de connexion à des systèmes informatiques quels qu'ils soient et de façon mal intentionnée ;
- Développer, installer, copier des programmes visant à exploiter des failles de sécurité, à contourner la sécurité, à saturer des ressources informatiques, à enregistrer des actions sur un matériel à l'insu de l'utilisateur ;
- Envoyer massivement des courriels à des fins autres qu'institutionnelles et sans autorisation préalable de l'Etablissement ;
- Utiliser abusivement les listes de diffusion de la messagerie ;
- Relier aux réseaux privés (hors réseaux de nomadisme) de l'établissement un quelconque matériel externe non déclaré par l'Etablissement et sans autorisation préalable de l'Administrateur ;
- Installer, créer, configurer, maintenir un serveur d'information internet sans autorisation préalable (http, ftp, dns, dhcp, …) ;
- Stocker des données, quels qu'en soient le volume et la nature, sur des supports externes hébergés par des Tiers, sans autorisation préalable de l'Administrateur ;
- Créer tout site internet accessible au public en ligne, ayant un lien direct ou indirect avec la Mission, sans information préalable de l'Etablissement s'agissant des Usagers étudiants, et sans l'autorisation préalable de l'Etablissement s'agissant des agents ;
- Accéder à des sites internet grâce aux outils de connexion et aux Ressources numériques mis à disposition par l'Etablissement, sans lien avec la Mission, de manière excessive dépassant la tolérance d'usage ;
- Participer à des forums en ligne ou accéder à des réseaux sociaux, en divulguant des informations inadéquates ou susceptibles de porter atteinte à la réputation de l'Etablissement, de toute personne ou de tout organisme, de violer le secret des correspondances ou la confidentialité de programmes de recherche ;
- Se déplacer munis d'ordinateur(s) portable(s) ou de support(s) amovible(s) confié(s) par l'Etablissement ou comportant des informations et données de l'Etablissement, sans prendre les précautions d'usage, à savoir : la conservation permanente sous contrôle, l'utilisation sans risque de divulgation d'information, le respect des règles d'hygiène informatique (écran de veille, codes d'accès, mise sous clé, chiffrement des données), la suppression de toutes données sensibles ou confidentielles avant tout déplacement à l'étranger.

8. Les sanctions et les textes de référence

8.1 Sanctions

L'établissement peut en cas de manquement grave aux règles et obligations définies dans la charte, pour tout Usager :

- Interdire provisoirement à titre conservatoire l'accès aux ressources numériques ;
- Déclencher des procédures disciplinaires et/ou pénales.

8.2 Principaux textes législatifs et sanctions se rapportant à la sécurité des systèmes d'information et à la protection des personnes

Sur la protection des personnes :

- Directive européenne 2002/58/CE du 12 juillet 2002 sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;
- Convention Européenne du 28 janvier 1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel ;

- Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi 2004-801 du 06 août 2004 ;
- Article 226-24 du Code Pénal : responsabilité des personnes morales des infractions aux dispositions de la loi sur les atteintes à la personnalité.

Sur la propriété intellectuelle :

- Article 335-2 du code de la Propriété intellectuelle : répression de la contrefaçon (jusqu'à 3 ans de prison et 300 000 Euros d'amende) ;
- Article 122-6 du code de la Propriété intellectuelle Sur l'atteinte aux droits de la personne résultant de fichiers ou traitements informatiques ;
- Articles 226-16 et suivants du Code pénal : violations de la Loi « Informatique et libertés » (jusqu'à cinq ans de prison et 300.000 € d'amende).

Sur les atteintes aux systèmes de traitement automatisé de données :

- Article 323-1 et suivants du code pénal: introduction frauduleuse, modification, suppression de données dans un système d'information ainsi que extraction, détention, reproduction ou transmission frauduleuse de données (cinq ans de prison et 75000 euros d'amende voire 7 ans et 100000 euros s'il s'agit de données à caractère personnel) ;

- Directive de la C.E.E. du 21 décembre 1988 sur l'harmonisation de la protection des logiciels.

Sur la violation des secrets et la prise de nom d'un tiers :

- Article 410-1 et 411-6 du nouveau Code Pénal : intérêts fondamentaux de la nation, secrets économiques et industriels ;
- Article 432-9 alinéa 1 et 226-15 du nouveau Code pénal: secret des correspondances (3 ans de prison et 45 000 Euros d'amende) ;
- Article 434-23 du Code pénal : usurpation d'identité (5 ans et 75 000 Euros d'amende) ;
- article 621-1 de la Propriété intellectuelle : secrets de fabrique (2 ans de prison et 30 000 Euros d'amende).

9. Diffusion et révision de la charte générale

Les technologies de l'information et leur cadre législatif évoluent fortement. L'Etablissement révisera dès lors que nécessaire la présente charte générale. Il s'engage à porter à la connaissance des Usagers toute révision de celle-ci au moyen des communications électroniques ou des portails intranet.

La présente charte reste annexée au règlement intérieur de l'Etablissement et consultable sur simple demande auprès de la Direction Générales des Services.

Toute information complémentaire peut être obtenue auprès de :

- la direction des systèmes d'information (DSI) ;
- le responsable de la sécurité des systèmes d'information (RSSI) ;
- le correspondant informatique et libertés (CIL) ;
- la direction des affaires juridiques (DAJI).

Recommandations poste de travail sur écran

Bérénice FAURY - Ergonome
Service de Santé au Travail UCA
Maison de la Vie Etudiante - Campus des Cézeaux
berenice.faury@uca.fr
04 73 40 52 42

I. Recommandation sur l'implantation du poste de travail

I.1. Environnement lumineux

Lumière
- Eviter les locaux aveugles (une vue sur l'extérieur) et privilégier un éclairage naturel (sans apport thermique excessif et sans éblouissement, éclairage zénithal dans bureau à proscrire). - Recommandation pour travail de bureau : ~ 300 lux (éclairage d'appoint si besoin). - Rajout de stores si gêne ou éclairement excessif (privilégier les stores à lamelles horizontales). - Eviter les sources lumineuses visibles dans un angle de 30° au-dessus du niveau des yeux. *N.b. : lorsque la distance entre la façade vitrée et les postes de travail est supérieur à 6m, l'éclairage naturel n'est plus assuré.*

I.3. Positionnement de l'agent

Ecran	Branchements informatiques / électriques
- Privilégier les écrans d'ordinateur positionnés perpendiculairement aux fenêtres. - En position assise, hauteur d'écran = hauteur des yeux (sauf en cas de port de verres progressifs dont la zone dédiée à la vision intermédiaire est basse = abaisser la hauteur de l'écran). - Eviter de placer un écran sous un luminaire plafonnier à éclairage direct. - Maintenir une distance écran-fenêtre supérieure ou égale à 1m50. - Eviter de positionner un écran juste devant un mur si le travail informatique est pratiqué sans alternance avec d'autres activités.	- Supprimer les fils au sol dans les zones de passage pour éviter le risque de chute (et faciliter le nettoyage des sols par les agents d'entretien). - Si besoin, prévoir des passe-câbles sous le bureau et des goulottes au sol.

Bérénice FAURY - Ergonome
Service de Santé au Travail UCA
Maison de la Vie Etudiante - Campus des Cézeaux
berenice.faury@uca.fr
04 73 40 52 42

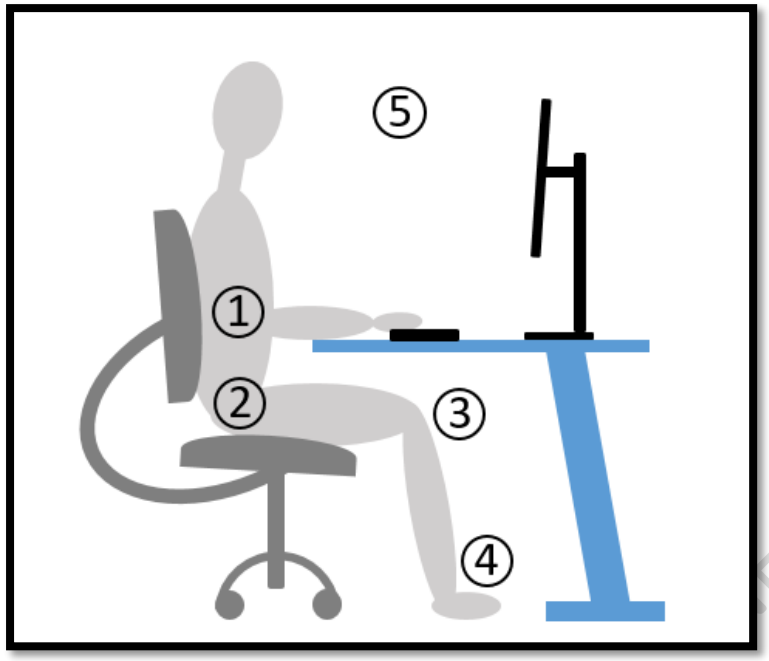
II. Mobilier

Bureau	Zone de rangements
- Privilégier les bureaux droits (pas d'arrondis). - Dimensions conseillées : profondeur 80 cm et largeur supérieure à 120 cm. Idéal entre 140 et 180 cm. - Plan de travail à définir en fonction de la variété des tâches et de la dimension des matériels. - Si besoin ajout d'un retour droit amovible (pouvant être mis à droite ou à gauche en fonction de l'utilisateur). - Supprimer les gênes au niveau des membres inférieurs (suppression du pied entre le bureau et son retour, caissons encombrants…) : l'utilisateur doit pouvoir se déplacer aisément avec son siège d'un bout à l'autre de son bureau. - Surface du bureau mat, pas de surface vitrée. - Exemples couleur bureau : chêne clair, érable, hêtre naturel… - Si remplacement d'un bureau, privilégier un modèle avec piétements réglables : permet de fixer la hauteur du bureau par rapport à la morphologie de l'agent. *(N.b. : hauteur standard d'un bureau environ 73 cm)* - Zone de débattement du siège bureautique : 1,2m2	- Privilégier les zones de rangements des éléments les plus utilisés à hauteur d'homme. - Privilégier les armoires dont la hauteur des plateaux de rangements peut être modifiée et possibilité d'intégrer des dossiers suspendus. - Bas et haut de l'armoire réservés pour stocker les éléments les moins consultés. Privilégier le bas pour stocker les éléments lourds.

Bérénice FAURY - Ergonome
Service de Santé au Travail UCA
Maison de la Vie Etudiante - Campus des Cézeaux
berenice.faury@uca.fr
04 73 40 52 42

III. Position assise

III.1. Conseils installation au poste



① Epaules détendues, avant-bras à l'horizontale, angle d'environ 90° au niveau des coudes. Mains, poignets et avant-bras dans le même alignement. Avant-bras en appui sur les accoudoirs ou sur le bureau.
Clavier : à environ 10 à 15 cm du bord du bureau, préférable de replier les patins.
Souris : juste à côté du clavier ou devant soi si le clavier est peu utilisé.

② Dos reposant sur le dossier. Au niveau des hanches : angle d'environ 90° à 110°.

③ Au niveau des genoux : angle d'environ 90°.
Le bord de l'assise ne doit pas compresser l'arrière du genou.

④ Pieds reposant à plat au sol (ou sur un repose-pieds). Au niveau des chevilles : angle de 90° environ.

⑤ Haut de l'écran doit être au niveau des yeux (si port de verres progressifs, abaissez l'écran). Distance yeux-écran = une longueur de bras. Positionnez dans la mesure du possible l'écran face à vous et perpendiculairement à la lumière naturelle.

→ Une bonne assise **ne remplace pas le besoin de se lever et marcher régulièrement** pour limiter les contraintes de la station assise prolongée. Nécessité de faire des pauses régulières lors du travail sur informatique et regarder au loin (plus de 5/6 mètres). Si possible alterner les tâches pour limiter le travail continu sur l'ordinateur.

Bérénice FAURY - Ergonome
Service de Santé au Travail UCA
Maison de la Vie Etudiante - Campus des Cézeaux
berenice.faury@uca.fr
04 73 40 52 42

III.2. Réglages recommandés d'un siège bureautique

- Assise : en hauteur et en profondeur
- Dossier : en hauteur

} Système synchrone : assise et dossier basculent simultanément et accompagnent l'utilisateur

- Si accoudoirs : privilégier les réglages en hauteur, profondeur, largeur + orientables pour les utiliser efficacement
- Piètements 5 branches et roulettes adaptées au type de sol

N.b. : Une phase de test par l'utilisateur est fortement recommandée avant acquisition.

→ Cf Plaquette sélection fauteuils UGAP

Bérénice FAURY - Ergonome
Service de Santé au Travail UCA
Maison de la Vie Etudiante - Campus des Cézeaux
berenice.faury@uca.fr
04 73 40 52 42