Centre Universitaire MAYOTTE

CONSEIL D'ADMINISTRATION
Séance du vendredi 27 septembre 2019
Délibération n°2019-27

Membres présents :

MEMBRES ELUS	MEMBRES EXTERIEURS	PERSONNALITÉS INVITEES
Collège A : M. Vincent EGEA. M. Nicolas LEROY (Visioconférence) **Collège B :** Mme Claire GOLLETY. M. Aurélien SIRI. **Collège C :** Mme Evelyne FONTAINE. M. Jean-Louis ROSE. **Collège des BIATSS :** M. Ridjal ABDOULAHI. Mme. Catherine FONTAINE. **Collège des USAGERS :** Mme Benoise BEN ATHMANE. M. Anil ABDOULKARIM représenté par Mme. Benoise BEN ATHMANE.	**Membres de droit :** Monsieur Benoit ROIG représenté par M. Aurélien SIRI M. Philippe AUGE représenté par M. Aurélien SIRI. **Représentant des activités économiques :** M. Zainal CHARAFOUDINE. **Représentant des organismes de salariés :** Monsieur Abdoul DAHALANI représenté par M. Zainal CHARAFOUDINE. **Personnalité extérieure :** Mme Anrafati COMBO représentée par M. Zainal CHARAFOUDINE.	M. Jean François COLOMBET, Préfet de Mayotte, Chancelier des universités, Mme Béatrice GILLE, Rectrice de l'Académie de Montpellier, Chancelière des universités, M. Gilles HALBOUT, Vice-Recteur de Mayotte, M. Zoubaïr Ben Jacques ALONZO, Directeur Général de la CCI de Mayotte, M. Jean-Marc LELEU, Directeur Régional des Finances Publiques de Mayotte, M. Fouad DOGGA, chargé de mission vie universitaire du Vice-Rectorat de Mayotte, Mme Onja ANDRIAMIANDRA, Directrice des affaires Financières, M. Fortuné DEMBI, Directeur des Ressources Humaines. **QUORUM ordinaire : 15/20** *(majorité des membres en exercice présente ou représentée)* **QUORUM budgétaire et statutaire : 10/20** *(majorité de l'effectif légal présente)*

Membre absents (excusés) *:* Monsieur Thierry GALARME (Représentant des organisations d'employeurs), M. Soibahadine IBRAHIM RAMADANI (Président du Conseil Départemental), M. Hugues DELOUTE (Personnalité extérieure), M. Nicolas LEROY (Représentant des professeurs d'université).

Invités absents (excusé) : M. Jean-François COLOMBET (Préfet de Mayotte – Chancelier des universités),

A l'ouverture de la séance, 9 personnes sont présentes sur les 20 membres composant le conseil d'administration, 5 procurations ont été données : M. Philippe AUGE (président de l'université partenaire de Montpellier) à M. Aurélien SIRI, Monsieur Benoit ROIG (président de l'université partenaire de Nîmes) représenté par M. Aurélien SIRI, M. Anil ABDOULKARIM (Représentant des usagers) représenté par Mme. Benoise BEN ATHMANE, Monsieur Abdoul DAHALANI (Représentant des organismes de salariés) représenté par M. Zainal CHARAFOUDINE, Mme Anrafati COMBO (Personnalité extérieure) représentée par M. Zainal CHARAFOUDINE.

Nature de l'acte :

Vu le règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/ce (règlement général sur la protection des données),
Vu la Convention n°108 du Conseil de l'Europe du 28 janvier 1980 pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel,
Vu le Code de l'éducation,

Vu le Code de la propriété intellectuelle,
Vu le Code pénal,
Vu la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,
Vu la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles,
Vu l'Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel,
Vu le décret n°2011-1299 du 12 octobre 2011 portant création du centre universitaire de formation et de recherche de Mayotte,
Vu le Règlement Intérieur du Centre Universitaire de Formation et de Recherche de Mayotte mis à jour des modifications votées au CA du 25 avril 2017

Le conseil d'administration après en avoir délibéré, décide :

Article unique

La Charte du bon usage des ressources du système d'information est approuvée.

Résultats du vote :

Nombre de votants..... : 15 Abstention..... : 0	Pour..... : 15 Contre..... : 0

Le président du conseil d'administration du CUFR
Zainal CHARAFFOUDINE

Le directeur du CUFR
Aurélien SIRI

Centre Universitaire de Mayotte
Le directeur

Envoi au contrôle de légalité le : *En application de l'article R.421-1 du code de justice administrative, le Tribunal administratif de Mayotte peut être saisi par voie de recours formé contre la présente délibération, dans un délai de 2 mois à compter de sa publication et de transmission au représentant de l'Etat à Mayotte.*	**Certifié exécutoire le :** *En application de l'article 21 du décret n° 2011-1299 précité, les délibérations du conseil d'administration sont exécutoires dans un délai de 15 jours suivant leur réception par le représentant de l'Etat à Mayotte.*

Centre Universitaire
MAYOTTE

Vu l'avis du CTE du 04/07/2019
Vu l'avis du CA du 27/09/2019

CHARTE DE BON USAGE DES RESSOURCES DU SYSTEME D'INFORMATION

SOMMAIRE

PREAMBULE

Le "système d'information" recouvre l'ensemble des ressources (personnels, procédures, matériel fixe et mobile, logiciel, données, réseaux de télécommunications) pouvant être mis à disposition par le CUFR de Mayotte.

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 définit les règles d'usages et de sécurité que le CUFR et les « utilisateurs » c'est-à-dire 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, s'engagent à respecter.

Engagements du CUFR

Le CUFR s'engage à diffuser la charte aux utilisateurs du système d'information.

Le CUFR met en œuvre les mesures nécessaires pour assurer la sécurité du système d'information et la protection des données à caractère personnel des utilisateurs.

Le CUFR facilite l'accès des utilisateurs aux ressources du système d'information pour un usage professionnel (et marginalement privé, voir paragraphe 2.01).

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 et de déontologie.

Les nouveaux personnels signeront la charte parmi leurs documents d'entrée. Les personnels en poste seront invités à indiquer par mail leur engagement à respecter cette charte.

Ce document aborde plusieurs points : les principes en matière de sécurité, la communication électronique via la messagerie et l'internet ainsi que les règles relatives à la traçabilité des informations techniques de connexion, aux droits de la propriété intellectuelle et la loi informatique et libertés, etc.

Dès lors qu'apparaitraient des doutes sérieux et fondés tant sur le contenu que sur l'utilisation d'une ressource de la part d'un agent, notamment au regard des règles mentionnées dans la charte, la direction se réserve le droit de suspendre les accès aux services de l'agent à titre conservatoire.

Article I. Champ d'application

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'ensemble du personnel du CUFR, utilisateur du système d'information de l'établissement.

Les usages relevant de l'activité des organisations syndicales et des étudiants sont régis par des chartes spécifiques.

Article II. Conditions d'utilisation du système d'information

Section 2.01 Utilisation professionnelle / privée

Les outils du système d'information (messagerie, internet…) sont destinés à des usages professionnels administratifs, pédagogiques et de recherche.

L'utilisation marginale du système d'information à titre privé doit être non lucrative et raisonnable, dans sa fréquence, sa durée et son volume.

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 explicitement à cet effet ou en mentionnant le caractère privé sur la ressource. La gestion et sauvegarde de ces données incombera à l'utilisateur.
Lors de son départ définitif de la structure 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'établissement.
L'utilisation du système d'information doit respecter la réglementation en vigueur, en particulier, la détention, diffusion et exportation d'images à caractère pédophile, ou la diffusion de contenus à caractère raciste ou antisémite est totalement interdite.
Par ailleurs, eu égard à la mission éducative de l'établissement, la consultation de sites de contenus à caractère pornographique depuis les locaux de l'établissement est interdite.

Section 2.02 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.

Section 2.03 Utilisation des ressources matérielles

Matériel affecté

L'utilisateur s'engage à respecter les matériels mis à sa disposition donc à :

- ne pas tenter de les ouvrir ou démonter

- ne pas forcer sur les prises et connecteurs
- ne pas débrancher les appareils connectés
- ne pas interrompre le fonctionnement normal du réseau ou des systèmes connectés
- les manipuler de façon à éviter les chutes ou heurts majeurs

Matériel prêté

L'utilisateur pourra se faire prêter certains équipements à condition :

- de faire partie du personnel ou de faire emprunter le matériel par un membre du personnel qui assurera la responsabilité de son usage
- de laisser sa carte d'identité (pour des prêts de courte durée, la copie de sa carte pour des prêts supérieurs à 1 mois)
- de remplir une fiche de prêt à durée limitée
- de s'engager à respecter le matériel, toute dégradation majeure pouvant donner lieu à facturation

Article III. Principes de sécurité

Section 3.01 Règles de sécurité d'accès au système d'information

Les codes d'accès constituent une mesure de sécurité essentielle, destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux ressources informatiques protégées un caractère personnel.

La bonne gestion de ses codes d'accès impose :

- de garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers, d'éviter de les écrire ou de faire mémoriser par le système ou les navigateurs
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.

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

De la part de l'établissement, limiter l'accès aux ressources pour lesquelles l'utilisateur est expressément habilité du fait des missions qu'il exerce et des circonstances de l'accès.

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'établissement ;
- ne pas installer, télécharger ou utiliser sur le matériel de l'établissement, des logiciels ou des données 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'établissement pour lutter contre les virus et les attaques par programmes informatiques ;

- ne pas déposer des données professionnelles sur un serveur externe et/ou ouvert au grand public ou sur le poste de travail d'un autre utilisateur sans analyse de risques préalable réalisée en concertation avec le RSSI (responsable de la sécurité du système d'information) et validée par le directeur de la structure ;
- assurer la protection des données sensibles et ne pas les transporter sans protection (telle qu'un chiffrement) sur des supports mobiles ;
- ne pas quitter son poste de travail sans l'avoir verrouillé ou s'être déconnecté.

Section 3.02 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.

Section 3.03 Mesures de contrôle de la sécurité

L'utilisateur est informé que pour effectuer la maintenance corrective, curative ou évolutive du système d'information, l'établissement se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition

L'établissement informe 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 pénale : *« 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 ».*

Article IV. Communication électronique

Section 4.01 Messagerie électronique

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

(a) Adresses électroniques

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

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'établissement : ces listes ne peuvent être utilisées sans autorisation explicite.

(b) Contenu des messages électroniques

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

Pour préserver le bon fonctionnement des structures de l'établissement des limitations peuvent être mises en place : dans ce cas, les termes en sont précisés et portés à la connaissance de l'utilisateur.

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…).

L'utilisation de la messagerie professionnelle par les organisations syndicales depuis le système d'information de l'établissement est régie par la charte relative aux usages syndicaux.

(c) Émission et réception des messages

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.

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

Section 4.02 Internet

Internet est un outil de travail ouvert à des usages professionnels (administratifs, pédagogiques et de recherche) et marginalement privés dans les conditions indiquées en section 2.01.

(a) Publication sur les sites internet et intranet de l'établissement

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

(b) Sécurité

L'Établissement 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.

(c) Téléchargements

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

L'établissement 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'établissement, codes malveillants, programmes espions …).

Article V. Traçabilité

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

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

Préalablement à cette mise en place, l'établissement 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.

Article VI. Respect de la propriété intellectuelle

L'établissement 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 :

- 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 écrite des titulaires de ces droits.

Article VII. Respect de la loi informatique et libertés

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

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 la loi «Informatique et Libertés».

En conséquence, tout utilisateur souhaitant procéder à une telle création devra en informer préalablement le directeur du système d'information de l'établissement qui prendra les mesures nécessaires au respect des dispositions légales.

Par ailleurs, conformément aux dispositions de cette loi, 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.

Ce droit s'exerce auprès du CRI via l'adresse : cri@univ-mayotte.fr

Article VIII. Limitation des usages

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation établis par la structure 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'établissement.

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

Article IX. Entrée en vigueur de la charte

La présente charte est annexée au règlement intérieur du CUFR et entre en vigueur à la date de signature par le directeur du CUFR.

Fait à Dembéni, le

Le Directeur du CUFR de Mayotte