MACS
Communauté de communes
Maremne Adour Côte-Sud

# CHARTE D'UTILISATION
# des Moyens & Outils Technologiques de l'Information et de la Communication (MOTIC)

SOMMAIRE

# 1 - INTRODUCTION

## 1.1 - LE CONTEXTE ET LES ENJEUX

Les différents outils technologiques utilisés offrent au personnel des collectivités territoriales et de leurs groupements une grande ouverture vers l'extérieur. Cette ouverture peut apporter des améliorations de performances importantes si l'utilisation de ces outils technologiques est faite à bon escient et selon certaines règles.

A l'inverse, une mauvaise utilisation de ces outils peut avoir des conséquences extrêmement graves. En effet, ils augmentent les risques d'atteinte à la confidentialité, à l'intégrité et à la sécurité des fichiers de données personnelles (virus, intrusions sur le réseau interne, vols de données), et de mise en jeu de la responsabilité.

De plus, mal utilisés, les outils informatiques peuvent aussi être une source de perte de productivité et de coûts additionnels.

L'application des nouvelles technologies d'information et de communication doit ainsi être compatible avec les impératifs de préservation du système d'information, de bon fonctionnement des services et les droits et libertés de chacun.

## 1.2 - L'OBJECTIF

La présente charte d'utilisation des MOTIC constitue le code de déontologie formalisant les règles légales et de sécurité relatives à l'utilisation de tout système d'information et de communication au sein de la Communauté de communes Maremne Adour Côte-Sud.

Le non-respect des règles énoncées dans la présente charte pourra entraîner le retrait du droit d'utilisation d'un outil, d'une application ou d'un matériel informatique/téléphonique et/ou des mesures d'ordre disciplinaire et/ou faire l'objet de poursuites pénales.

## 1.3 - LE CHAMP D'APPLICATION

La présente charte s'applique à l'ensemble du personnel tous statuts confondus, ainsi qu'au personnel temporaire, élus et administrateurs. Elle s'applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques de l'établissement. Tout contrat avec un prestataire extérieur devra y faire référence et comporter comme annexe la présente charte.

Dès l'entrée en vigueur de la présente charte, chaque agent de l'établissement s'en verra remettre un exemplaire. Il devra en prendre connaissance et s'engager à la respecter (cf. Récépissé).

# 2 - LES RÈGLES GÉNÉRALES D'UTILISATION

Les utilisateurs sont présumés adopter un comportement responsable, s'interdisant notamment toute tentative d'accès à des données ou à des sites qui leurs seraient interdits, en vertu des lois et règlements en vigueur.

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie et s'engage à ne pas effectuer d'opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement du réseau. Il doit en permanence garder à l'esprit que c'est sous le nom de l'établissement qu'il se présente sur Internet et doit se porter garant de l'image de l'institution.

Au même titre que pour le courrier, le téléphone ou la télécopie, chacun est responsable des messages envoyés ou reçus, et doit utiliser la messagerie dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues et des règles élémentaires de courtoisie et de bienséance.

## 2.1 - LES DROITS ET LES DEVOIRS DES UTILISATEURS

### *2.1.1 - UN ACCÉS AUX RESSOURCES RÉGLEMENTÉ*

Toute personne travaillant (agent) ou détenant un mandat (élu) dans l'établissement dispose d'un droit d'accès au système d'information. Ce droit d'accès est :

- strictement personnel ;
- incessible.

### *2.1.2 - UNE UTILISATION PROFESSIONNELLE DES RESSOURCES*

Les ressources informatiques mises à disposition constituent un outil de travail nécessaire. Chaque utilisateur doit adopter une attitude responsable et respecter les règles définies sur l'utilisation des ressources et notamment :

- respecter l'intégrité et la confidentialité des données ;
- ne pas perturber la disponibilité du système d'information ;
- ne pas stocker ou transmettre d'information portant atteinte à la dignité humaine ;
- ne pas marquer les données exploitées d'annotations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et images de chacun ou faisant référence à une quelconque appartenance, à une ethnie, religion, race ou nation déterminée (loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « informatique et libertés ») ;
- respecter le droit de propriété intellectuelle : non reproduction et/ou non diffusion de données soumises à un droit de copie non-détenu, interdiction de copie de logiciel sans licence d'utilisation ;
- ne pas introduire de « ressources extérieures » matérielles ou logicielles qui pourraient porter atteinte à la sécurité du système d'information ;
- respecter les contraintes liées à la maintenance du système d'information.

### *2.1.3 - UNE UTILISATION NON PROFESSIONNELLE DES RESSOURCES*

L'utilisation des ressources professionnelles à des fins personnelles ou privées est toléré selon les modalités suivantes :

- l'usage doit rester raisonné, occasionnel et ne pas contrevenir à la loi ;
- le stockage de données privées sur les équipements de l'établissement est toléré et ne saurait excéder une volumétrie totale de 250 Mo par agent.
- le stockage de dossiers et fichiers privés doit être explicite et réalisé dans un dossier intitulé « PERSONNEL » ou « PRIVÉ » ;
- le stockage de données privées doit être temporaire : aucun dossier ou fichier ne saurait être stocké pour une durée supérieure à 5 jours ouvrables.

Ces données devront être stockées dans l'espace de stockage personnel nommé *prénom.nom (U :)* :

#### *2.1.4 - CONFIDENTIALITÉ DES DONNÉES PRODUITES PAR L'ÉTABLISSEMENT*

Les données produites par ou pour l'établissement sont confidentielles et propriétés dudit établissement. Elles ne pourront être diffusées qu'avec l'accord exprès de l'autorité territoriale.

L'utilisation de ces données à des fins personnelles pourra être sanctionnée.

## 2.2 - LES DROITS ET LES DEVOIRS DE L'ÉTABLISSEMENT

L'établissement doit veiller à la disponibilité et à l'intégrité du système d'information. En ce sens, il s'engage à :

- mettre à disposition les ressources informatiques matérielles et logicielles nécessaires au bon déroulement de la mission des utilisateurs ;
- mettre en place des programmes de formations adaptés et nécessaires aux utilisateurs pour une bonne utilisation des outils ;
- informer les utilisateurs des diverses contraintes d'exploitation (interruption de service, maintenance, modification de ressources, etc.) du système d'information susceptible d'occasionner une perturbation ;
- effectuer les mises à jour nécessaires des matériels et des logiciels composant le système d'information afin de maintenir le niveau de sécurité en vigueur dans le respect des règles d'achat et des budgets alloués ;
- respecter la confidentialité des « données utilisateurs » auxquelles il pourrait être amené à accéder pour diagnostiquer ou corriger un problème spécifique ;
- définir les règles d'usage de son système d'information et veiller à leur application ;
- pour des nécessités de gestion technique, respecter les engagements budgétaires, garantir la sécurité et l'intégrité des ressources matérielles et logicielles de l'établissement. L'utilisation de ces ressources pourra être enregistrée, analysée et contrôlée dans le respect de la législation applicable, et notamment de la loi informatique et libertés.

La nature et la finalité de ces enregistrements seront détaillées indépendamment selon les ressources dans les chapitres suivants.

Conformément aux règles édictées par la Commission nationale de l'informatique et des libertés (CNIL), l'employeur peut accéder aux fichiers et dossiers identifiés comme « personnels » ou « privés » :

- en présence du salarié ou après l'avoir invité à être présent ;
- en l'absence du salarié et sans l'en informer, en cas d'évènement ou de risque particulier pour l'organisation (risque de sécurité, continuité de service, etc.).

Par défaut, les fichiers stockés sur les postes de travail et les serveurs ont un caractère professionnel et l'employeur peut y accéder librement.

### 2.3 - LES SANCTIONS

La loi, les textes réglementaires (cf. annexes 1 et 2) et la présente charte définissent les droits et obligations des personnes utilisant les ressources informatiques.

Tout utilisateur du système d'information de l'établissement n'ayant pas respecté la loi et les règlements en vigueur pourra être poursuivi pénalement (cf. annexes 1 et 2).

En outre, tout utilisateur ne respectant pas les règles définies dans la présente charte est passible de mesures qui peuvent être internes à l'établissement (retrait du droit d'utilisation d'un outil, d'une application ou d'un matériel informatique/téléphonique) et/ou de sanctions disciplinaires proportionnelles à la gravité des manquements constatés par l'autorité territoriale.

### 2.4 - LES ÉVOLUTIONS

Avant son entrée en vigueur, la présente charte a été soumise à l'avis du comité technique commun placé auprès de la Communauté de communes et approuvée par délibération de l'organe délibérant de l'établissement. Elle pourra être complétée ou modifiée selon les mêmes formes ; dans ce cas, l'avis du comité technique sera à nouveau demandé.

## 3 - LES POSTES INFORMATIQUES

Cette présente partie a pour objectif d'établir les règles d'utilisation des postes.

Un ensemble « matériels - système d'exploitation - logiciels » est mis à disposition de chaque utilisateur :

- matériel : unité centrale, écran, clavier, souris… ;
- système d'exploitation : Windows (SEVEN, 8, 10, MAC OS) ;
- logiciel : pack bureautique, logiciels de communication, logiciels de gestion, applications spécifiques.

Le matériel informatique est fragile, il faut en prendre soin et redoubler d'attention pour les écrans plats. Les supports amovibles (disquettes, CD ROM, clé USB, etc.) provenant de l'extérieur doivent être soumis à un contrôle antivirus préalable.

Toute installation logicielle est à la charge de la personne compétente et désignée par l'autorité territoriale.

En cas d'absence momentanée, l'utilisateur doit verrouiller son PC (Ex. : maintenir enfoncées les touches « Ctrl + Alt + Suppr » et cliquer sur « Verrouiller l'ordinateur »).

En cas d'absence prolongée, l'utilisateur doit quitter les applications et verrouiller son PC.

A la fin de sa journée de travail, l'utilisateur doit quitter les applications, arrêter le système par arrêt logiciel, éteindre l'écran et l'imprimante.

Un premier niveau de sécurité consiste à utiliser des mots de passe sûrs non communiqués à des tierces personnes et régulièrement modifiées (deux fois par an).

L'utilisateur n'usurpera pas l'identité d'autrui.

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde quotidienne des informations.

L'utilisateur doit signaler tous dysfonctionnements ou anomalies au service ou référent informatique.

L'utilisateur doit procéder régulièrement à l'élimination des fichiers non-utilisés et à l'archivage dans le but de préserver la capacité de mémoire et la vitesse de restauration en cas de panne majeure.

# 4 - LOGICIELS MÉTIERS ET TÉLÉSERVICES

Sont qualifiés de « logiciels métiers » les logiciels de gestion de l'établissement. A titre d'exemple, les outils système d'information géographique, gestion de projets, gestion de production, gestion des congés, gestion financière, gestion de plannings, etc.

Chaque utilisateur doit être authentifié pour accéder aux logiciels métiers avec les droits qui lui ont été attribués par l'administrateur du logiciel métier. L'authentification se fait via un compte utilisateur nominatif, comportant un identifiant et un mot de passe.

L'utilisateur doit respecter les règles d'usage du logiciel métier pour lesquels les droits lui sont attribués.

L'utilisateur n'est pas autorisé à utiliser un logiciel métier non validé par son responsable de service pour traiter des données de l'établissement.

Dans le cas où les outils métiers engendreraient une géolocalisation, les fonctionnalités de géolocalisation sont utilisées uniquement à des fins de suivi d'activités (géolocalisation d'un incident de voirie, optimisation des trajets, dispositif d'alerte pour travailleurs isolés, etc.). Les utilisateurs disposent des accès nécessaires à l'arrêt de la géolocalisation en dehors de leurs heures de travail.

# 5 - LA MESSAGERIE

Cette présente partie a pour objectif d'établir les règles d'utilisation de la messagerie électronique.

## REGLES D'UTILISATION

L'utilisation de la messagerie est réservée à des fins professionnelles. Néanmoins, il est toléré, en dehors des heures de travail, un usage modéré de celle-ci pour des besoins personnels et ponctuels.

L'utilisateur veillera à ne pas ouvrir les courriels dont le sujet paraîtrait suspect.

Les courriels à caractère privé et personnel doivent être identifiés comme « privé » dans l'objet du message ou dans le nom du répertoire de stockage. Ils sont ainsi couverts par le secret de la correspondance, comme les conversations téléphoniques.

Afin de garantir la sécurité et le bon fonctionnement du système de messagerie, les données de connexion au serveur de messagerie pourront être enregistrées, conformément au référentiel relatif aux traitements de données personnelles mis en œuvre aux fins de gestion des ressources humaines adopté le 21 novembre 2019 par la CNIL.

L'utilisateur s'engage à ne pas envoyer, en dehors des services de l'établissement, des informations professionnelles nominatives ou confidentielles, sauf si cet envoi revêt un caractère professionnel.

L'utilisateur soigne la qualité des informations envoyées à l'extérieur et s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine ou à la vie privée de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.

L'utilisateur signera tout courriel professionnel.

L'utilisateur doit vérifier la liste des destinataires et respecter les circuits de l'organisation ou la voie hiérarchique le cas échéant.
L'utilisateur doit éviter de surcharger le réseau d'informations inutiles. Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier « éléments supprimés » doit être vidé périodiquement.

En cas d'absence prévisible, l'utilisateur devra mettre en place un message automatique d'absence indiquant la date de retour prévue. Un agent du service doit pouvoir gérer les messages pendant son absence.

Une équivalence juridique peut être établie entre le courrier électronique et le courrier sur support papier dans les conditions déterminées par le code civil.

# 6 - L'INTERNET

Cette présente partie a pour objectif d'établir les règles d'utilisation d'Internet.

## REGLES D'UTILISATION

L'utilisation d'Internet est réservée à des fins professionnelles et/ou syndicales dans le cadre de l'exercice des décharges d'activité et autorisations spéciales d'absence.

Néanmoins, il est toléré en dehors des heures de travail un usage modéré de l'accès à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel.

L'utilisateur s'engage, lors de ses consultations Internet, à ne pas se rendre sur des sites portant atteinte à la dignité humaine (pédopornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée).

Le téléchargement gratuit, en tout ou partie, de données numériques soumises aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.) est strictement interdit.

Le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet est interdit.

Tout abonnement payant à un site web ou à un service via Internet doit faire l'objet d'une autorisation préalable de l'autorité territoriale.

En conformité avec les lois et règlements en vigueur, pour éviter d'éventuels abus, les accès entrants et sortants seront administrés afin de ne laisser passer que les usages professionnels, syndicaux, et personnels n'entravant pas l'accès professionnel (consultation sites internet, mails, téléchargement professionnels). Tout usage non autorisé par les présentes règles pourra faire l'objet d'une dérogation sur demande, si celle-ci n'interfère pas avec les règles de bon usage des outils informatiques, et la qualité de service attendue.

L'autorité territoriale peut procéder, à tout moment, à l'enregistrement des données de connexions pour assurer la sécurité et le bon fonctionnement des applications et réseaux informatiques, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des agents, conformément au référentiel relatif aux traitements de données personnelles mis en œuvre aux fins de gestion des ressources humaines précité.

Aucun contrôle en temps réel ne sera réalisé sur ces données de connexions, leur but étant uniquement de servir de preuves en cas de problème.

# 7 - LE TÉLÉPHONE

Cette présente partie a pour objectif d'établir les règles d'utilisation du téléphone.

## REGLES D'UTILISATION

L'utilisation des téléphones fixes et portables est réservée à des fins professionnelles.

L'utilisation des téléphones portables est interdite depuis et/ou vers l'étranger, sauf dérogation expresse.

L'utilisation des téléphones portables à des fins personnelles doit rester occasionnelle et discrète.

En cas d'absence, l'utilisateur doit effectuer un renvoi sur le poste d'un autre agent du service ou sur l'accueil téléphonique.

L'agent qui quitte définitivement l'établissement doit préalablement restituer le téléphone portable professionnel. L'utilisateur doit veiller à soigner sa présentation lors d'un appel pour faciliter son identification et/ou son service.

Afin de maitriser les dépenses liées à la téléphonie, l'autorité territoriale peut procéder au contrôle de l'ensemble des appels émis, en cas d'utilisation manifestement abusive du téléphone par un agent.

Les données contrôlables sont les suivantes :

- numéros de téléphone appelés ;
- services utilisés ;
- opérateurs appelés ;
- nature de l'appel (local, départemental, national, international) ;
- durée, date et heure de début et de fin d'appel ;

Elles pourront être contrôlées pendant une durée de 1 an.

Afin de sécuriser la flotte de téléphones mobiles, une application de type EMM (Enterprise Mobility Management) est déployée. Les fonctionnalités de l'outil sont les suivantes :

- mettre à disposition de manière automatisée un catalogue d'applications présélectionnées ;
- réaliser des maintenances à distance sur les smartphones après accord de l'utilisateur. Cet accord est matérialisé par une demande diffusée sur le smartphone. Après accord, la consultation de l'écran ou la prise en main par la direction des Systèmes d'Informations est possible ;
- bloquer ou réinitialiser, en cas de perte ou de vol, le contenu du smartphone afin d'empêcher tout accès aux données professionnelles contenues dans l'équipement.

# 8 - MATÉRIELS DE PRÊT

Les services peuvent être amenés à solliciter du prêt de matériel pour des évènements spécifiques.

Lors du prêt d'équipement, l'utilisateur à qui est remis le matériel doit renseigner et signer un formulaire de prêt de matériel auprès de la Direction des Systèmes d'Informations actant la remise des équipements nomades ou encore le prêt d'un matériel spécifique pour la tenue d'un évènement (écran blanc, vidéoprojecteur, etc.).

Il en assure la garde et la responsabilité et doit informer la direction des Systèmes d'Informations en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches, telles que la déclaration de vol et le dépôt de plainte auprès des officiers de police judicaire compétents.

Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements. Le retour du matériel fait l'objet d'un formulaire de fin de prêt de matériel.

# 9 - DROIT À LA DÉCONNEXION DES AGENTS

Les outils numériques exigent de nouvelles protections pour garantir l'effectivité du droit en matière de temps de travail, de repos et de santé des agents. L'enjeu est de garantir un réel droit à la déconnexion par rapport à la vie professionnelle afin de préserver la vie privée et la santé. Pour obtenir ce droit effectif à la déconnexion, il est nécessaire d'encadrer l'usage des outils numériques.

Afin de mieux respecter les temps de repos et de congés, ainsi que la vie personnelle et familiale des agents, l'article 55 de la loi n° 2016-1088 du 8 août 2016, dite « Loi Travail » crée un droit à la déconnexion. Bien que cette obligation ne concerne pas les employeurs publics, l'établissement s'engage, dans le prolongement de la circulaire du 31 mars 2017 relative à l'application des règles en matière de temps de travail dans les trois versants de la fonction publique, à travers les mesures contenues dans la présente charte, à mettre en place les mesures participant de ce « droit à la déconnexion ».

Qu'est-ce que cela implique ?

La loi Travail impose aux employeurs, depuis le 1er janvier 2017, de réguler l'usage des moyens et outils technologiques d'information et de communication.

L'instauration d'un droit à la déconnexion vise à garantir l'effectivité du droit au repos.

Aussi est-il prévu la mise en place par l'établissement des dispositifs de régulation de l'utilisation des outils numériques, en vue d'assurer le respect des temps de repos et de congés ainsi que de la vie personnelle et familiale.

Ces mesures comprennent :

- des modules de formation aux Escales Numériques (exemple : module de formation au télétravail, etc.) ;
- des modules de formation à destination des agents et des managers dans le cadre du télétravail ;
- etc.

### 9.1 - DES ACTIONS D'INFORMATION ET DE FORMATION

Des actions de sensibilisation des agents et des managers seront menées concernant l'impact de l'usage des outils numériques sur les agents de l'établissement.

Des temps de formations seront organisés pour tous les agents à l'usage des outils numériques, sur l'hyper connexion et la surcharge d'informations.

### 9.2 - DES ACTIONS DE PREVENTION DES RISQUES PROFESSIONNELS (CHSCT)

Le comité d'hygiène, de sécurité et des conditions de travail (CHSCT) sera associé au projet du « droit à la déconnexion » : le CHSCT peut apporter ses compétences spécifiques et proposer des mesures de prévention organisationnelles, techniques et humaines à intégrer dans la présente charte.

## 10 - RÈGLEMENT GÉNÉRAL DE LA PROTECTION DES DONNÉES

Les données répondant aux conditions de la loi n° 78-17 du 6 janvier 1978 ont fait l'objet d'une déclaration auprès de la CNIL selon les modalités en vigueur.

Les utilisateurs sont informés que les données à caractère personnel les concernant sont conservées pendant toute la durée de leur relation contractuelle et des délais en matière de prescription.

Conformément à la loi, les utilisateurs sont informés qu'ils disposent d'un droit d'accès et de rectification relatif à l'ensemble des informations les concernant.

Les utilisateurs sont également informés que, pour des motifs légitimes, ils peuvent s'opposer au traitement des données personnelles les concernant.

Les systèmes d'informations, du fait de leurs champs de compétences, sont soumis de plein droit au RGPD et à la désignation d'un Délégué à la Protection de Données personnelles (DPD appelé aussi DPO).

En effet, les données traitées par les systèmes d'informations de l'établissement correspondent bien à l'alinéa 15 de l'article 4 : Définition, du Règlement de l'Union Européenne du 27 avril 2016 relatif au RGPD.

De plus, les systèmes d'informations relèvent également, en matière de traitement de la donnée personnelle à caractère particulier dite également sensible, de l'article 9 du RGPD en ses alinéas 2b et 2h.

Au sein de la communauté de communes, un Délégué à la Protection des Données (DPD) est nommé. Ses missions sont les suivantes :

- informer et conseiller le responsable du traitement ou les collaborateurs qui procèdent au traitement sur les obligations qui leur incombent en vertu du RGPD et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données;
- contrôler le respect du RGPD en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant;
- dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35 du RGPD;
- coopérer avec l'autorité de contrôle à savoir la CNIL;
- faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet.

# 11 - PROCÉDURE APPLICABLE EN CAS D'ABSENCE PROLONGÉE OU LORS DU DÉPART D'UN AGENT

## 11.1 - ABSENCE PROLONGEE

En cas d'absence prolongée d'un utilisateur (arrêt de travail, etc.) excédant 3 mois, l'établissement pourra demander à l'utilisateur de restituer le matériel mis à sa disposition : ordinateur, téléphone portable, etc.

## 11.2 - DEPART EN FIN DE CONTRAT OU MISE EN DISPONIBILITE

Lors de son départ, l'utilisateur doit restituer au service informatique les équipements et les identifiants mis à sa disposition.

Il doit préalablement effacer ses fichiers de données privées. Toute copie de documents professionnels doit être autorisée par le responsable de service.

Les comptes et les données personnels de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après sa fin de contrat ou sa date de mise en disponibilité.

# 12 - ÉVOLUTION ET MODIFICATION DE LA PRÉSENTE CHARTE

Les modifications et extensions prévues du système d'information et de communication électronique qui affectent de manière perceptible l'objet de la présente charte seront communiquées aux délégués du personnel et au Délégué à la Protection des données.
La charte d'utilisation des moyens et outils technologiques de l'information et de la communication sera modifiée en conséquence et, le cas échéant, après consultation et information des délégués du personnel, sera soumis à l'approbation de l'organe délibérant avant communication au personnel de l'établissement.

La présente Charte a été approuvée par délibérations du conseil communautaire du .....

Pour MACS,

Le président,

Pierre Froustey

# 13 - GLOSSAIRE

(À compléter, le cas échéant, par l'autorité territoriale lors de toute modification)

SYSTEME D'INFORMATION :

Ensemble des éléments participant à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'établissement.

RESSOURCES INFORMATIQUES :

- les matériels ;
- les logiciels et les procédures ;
- les données et les fichiers.

INTERNET :

Interconnexion mondiale de réseaux reposant sur un protocole appelé « Internet » et dont les applications les plus utilisées sont le courriel et les consultations de sites (Web).

INTRANET :

Utilisation des technologies liées à Internet au sein d'un réseau local. Les principaux intérêts sont de faciliter et de rendre plus conviviale l'accès aux données par l'utilisation du navigateur et de la messagerie interne.

EXTRANET :

On peut dire que c'est un « Intranet » étendu à des utilisateurs extérieurs qui, n'étant pas situés sur le réseau local, seront soumis à un accès sécurisé.

COURRIEL :

Message électronique.

RÉSEAU :

Ensemble d'ordinateurs et de machines informatiques qui communiquent grâce à une technique commune de transmission.

PÉRIPHÉRIQUES :

Matériels connectés à un poste de travail ou directement sur le réseau local (exemples : imprimante, scanners…).

ADMINISTRATEUR :

Membre du service informatique en charge des ressources informatiques. Il est soumis au secret professionnel en ce qui concerne les données personnelles ou confidentielles dont il pourrait être amené à prendre connaissance dans l'exercice de ses fonctions.

CONNEXION ENTRANTE ou SORTANTE :

Flux réseau allant respectivement de l'extérieur (internet) vers l'intérieur du réseau de l'établissement, ou du réseau interne de l'établissement vers l'extérieur (internet)

DOSSIER / FICHIER PARTAGÉ :

Dossier ou fichier d'un agent dont l'accès est possible à plusieurs utilisateurs (exemple : le dossier commun) ;

DOSSIER / FICHIER PERSONNEL :

Dossier ou fichier d'un agent contenant des données et informations professionnelles dont il est le seul à disposer des accès (exemple le dossier U :) ;

DOSSIER / FICHIER PRIVÉ :

Dossier ou fichier d'un collaborateur contenant des données et informations personnelles ou privées et devant impérativement être identifié comme tel.

# 14 - RÉCÉPISSÉ CHARTE D'UTILISATION DES MOTIC

Je soussigné(e) :

Nom :.....

Prénom :.....

Service : .....

Fonction : .....

utilisateur des moyens et outils technologiques de l'information et de la communication de l'établissement ....., déclare avoir pris connaissance de la présente charte et m'engage à la respecter.

Fait à ..... Le .....

Signature

Fait en deux exemplaires :

- un pour l'intéressé ;
- un pour l'établissement.

# 15 - ANNEXE 1 - LES BASES LÉGALES

L'utilisateur doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n° 84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale.

Cette présente partie a pour objectif d'informer les utilisateurs des textes législatifs et réglementaires dans le domaine de la sécurité des systèmes d'information.

A - Textes de référence

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

Elle a notamment pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.

Loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle

Elle interdit à l'utilisateur d'un logiciel toute reproduction de celui-ci autre que l'établissement d'une copie de sauvegarde.

Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

Loi n° 2004-575 du 21/06/2004 pour la confiance dans l'économie numérique.

Elle est destinée à favoriser le développement du commerce par Internet, en clarifiant les règles pour les consommateurs et les prestataires aussi bien techniques que commerciaux.

Code des relations entre le public et l'administration

Code de la propriété intellectuelle

Code pénal (articles 323-1 à 323-8 issus de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique).

Cette loi, dite de GODEFRAIN, vise à lutter contre la fraude informatique en réprimant :

- les accès ou maintien frauduleux dans un système d'information
- les atteintes accidentelles ou volontaires au fonctionnement
- la falsification des documents informatiques et leur usage illicite
- l'association ou l'entente en vue de commettre un de ces délits

Code pénal (article 432-9 relatif aux atteintes au secret des correspondances)

Code civil (articles 1316-1 et 1367)

Le droit disciplinaire

**Loi n° 84-53 du 26 janvier 1984 modifiée** (art. 89 et 90) et le décret n° 89-677 du 18 septembre 1989 relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux.

**Décret n° 92-1194 du 4 novembre 1992** (art. 6) fixant les dispositions communes applicables aux fonctionnaires stagiaires de la fonction publique territoriale.

**Décret n° 88-45 du 15 février 1988** (art. 36 et 37) relatif aux agents non titulaires.

**Décret n° 91-298 du 20 mars 1991** (art. 15) relatif aux agents à temps non complet.

B - Le code pénal

Code pénal Livre 3 Titre 2 Chapitre III : Des atteintes aux systèmes de traitement automatisé de données.

Article 323-1 : (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre

2000 en vigueur le 1er janvier 2002)

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15.000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de

30.000 euros d'amende. »

Article 323-2 : (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre

2000 en vigueur le 1er janvier 2002)

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45.000 euros d'amende. »

Article 323-3 : (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre

2000 en vigueur le 1er janvier 2002)

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 45.000 euros d'amende. »

Article 323-4 :

« La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

Article 323-5 :

« Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1º L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26.

2º L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.

3º La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution.

4º La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés.

5º L'exclusion, pour une durée de cinq ans au plus, des marchés publics.

6º L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés.

7º L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35. »

Article 323-6 :

« Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont :

1º L'amende, suivant les modalités prévues par l'article 131-38.

2º Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2º de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise. »

Article 323-7 :

« La tentative des délits prévus par les articles 323-1 à 323-3 est punie des mêmes peines. »