Envoyé en préfecture le 25/06/2018
Reçu en préfecture le 25/06/2018
ID : 040-200009868-20180613-13062018D06-DE

Centre intercommunal d'action sociale
Séance du 13 juin 2018
Délibération n° 13062018D06

CENTRE INTERCOMMUNAL D'ACTION SOCIALE DE MACS
SÉANCE DU MERCREDI 13 JUIN 2018 À 18 HEURES
SALLE DANGOU LESCOUZÈRES
(sur convocation du 7 juin 2018)

Président
Nombre de conseillers : 9
Nombre de membres nommés : 9
Présents : 10
Absents représentés : 6
Absents excusés : 3

REGISTRE DES DÉLIBÉRATIONS DE LA SÉANCE
DU CONSEIL D'ADMINISTRATION DU CIAS DE MACS
DU 13 JUIN 2018

L'an deux mille dix-huit, le treize du mois de juin à 18 heures, le conseil d'administration du Centre intercommunal d'action sociale de la Communauté de communes Maremne Adour Côte-Sud, dûment convoqué le 7 juin 2018, s'est réuni en session ordinaire, au siège de MACS à Saint-Vincent de Tyrosse, sous la présidence de Madame Frédérique Charpenel.

Présents :
Mesdames Frédérique CHARPENEL, Sylvie DE ARTECHE, Maïté GRAFF, Françoise TROCCARD et Pierrette MICHELENA ;
Messieurs Alain LAVIELLE, Alain JEAN, Pierre LAFFITTE, Jérôme PETITJEAN et Jean-Paul TOURNIER.

Absents représentés :
Madame Rosa DI MURO a donné pouvoir à Madame Frédérique CHARPENEL, Madame Corine LAFITTE a donné pouvoir à Monsieur Alain LAVIELLE, Madame Nelly BETAILLE a donné pouvoir à Madame Sylvie DE ARTECHE, Monsieur Michel PENNE a donné pouvoir à Madame Françoise TROCCARD, Monsieur Benoît DARETS a donné pouvoir à Monsieur Jérôme PETITJEAN et Monsieur Pierre ATHANASE a donné pouvoir à Monsieur Alain JEAN.

Absents excusés :
Messieurs Pierre FROUSTEY, Yves MONGROLLE et Pascal SCHWINDOWSKY.

OBJET : APPROBATION DE LA CHARTE D'UTILISATION DES MOYENS ET OUTILS TECHNOLOGIQUES DE L'INFORMATION ET DE LA COMMUNICATION (MOTIC)

Rapporteur : Madame Frédérique CHARPENEL

Les différents outils technologiques utilisés offrent au personnel des collectivités territoriales et de leurs groupements, une grande liberté et ouverture vers l'extérieur. Si cette ouverture peut être source d'amélioration et de performances importantes, à condition que l'utilisation de des outils soit faite à bon escient et selon certaines règles, une mauvaise utilisation ces derniers peut emporter des conséquences extrêmement graves pour les agents. En effet, les outils technologiques augmentent les risques d'atteinte à la confidentialité, à l'intégrité et à

Envoyé en préfecture le 25/06/2018
Reçu en préfecture le 25/06/2018
ID : 040-200009868-20180613-13062018D06-DE

la sécurité des fichiers de données personnelles (virus, intrusions sur le réseau interne, vols de données), et peuvent, le cas échéant, mettre en jeu la responsabilité des agents. De surcroît, mal utilisés, les outils informatiques peuvent également être une source de perte de productivité et de coûts additionnels.

L'application des nouvelles technologies d'information et de communication doit être compatible avec les impératifs de préservation du système d'information, de bon fonctionnement des services et les droits et libertés de chacun. Aussi, 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. Pour obtenir un droit effectif à la déconnexion, l'usage des outils numériques doit être encadré.

Dans ce cadre, il convient d'adopter un « code déontologique » propre à la Communauté de communes, 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 et du Centre intercommunal d'action sociale (CIAS) de MACS. En outre, afin de mieux respecter les temps de repos et de congés, ainsi que la vie personnelle et familiale des agents, l'établissement s'engage à mettre en place les mesures participant de ce « droit à la déconnexion ».

1. Champ d'application

La charte d'utilisation des MOTIC, dont le projet est annexé à la présente, s'applique à l'ensemble du personnel, quel que soit son statut, au personnel temporaire et aux administrateurs du CIAS. Elle est également applicable à tout prestataire extérieur ayant accès aux données et aux outils informatiques de l'établissement. Dans cette mesure, tout contrat conclu avec un prestataire extérieur devra se référer à cette dernière.

Dès l'entrée en vigueur de la charte d'utilisation des MOTIC, chaque agent du CIAS de MACS s'en verra remettre un exemplaire et devra en prendre connaissance tout en s'engageant à la respecter à travers la remise d'un récépissé.

Une version de la charte est déclinée à l'attention des administrateurs, dès lors qu'ils bénéficient d'une mise à disposition, à titre individuel, de moyens informatiques et de télécommunications nécessaires à l'exercice de leurs mandats, conformément aux dispositions de l'article L. 2121-13 du code général des collectivités territoriales.

2. Règles générales d'utilisation des MOTIC

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 travers le respect de la charte d'utilisation des MOTIC, 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 d'établissement qu'il se présent sur Internet et doit se porter garant de l'image de l'institution.

A travers l'adoption et le respect de la charte d'utilisation des MOTIC, et au même titre que pour le courrier, le téléphone ou la télécopie, tout utilisateur est responsable des messages envoyés ou reçus, et doit utiliser la messagerie dans le respect de la hiérarchie le cas échéant, des missions et fonctions qui lui sont dévolues et de règles règlementaires de courtoisie et de bienséance.

Enfin, la charte reconnait le droit à la déconnexion pour les agents.

3. Sanctions

La charte d'utilisation des MOTIC, annexée à la présente, crée des droits et des obligations pour les utilisateurs et prestataires extérieurs utilisant les ressources informatiques. Le non-respect des obligations les expose à des sanctions pénales et à des poursuites disciplinaires le cas échéant.

Le CONSEIL D'ADMINISTRATION,

Envoyé en préfecture le 25/06/2018
Reçu en préfecture le 25/06/2018
ID : 040-200009868-20180613-13062018D06-DE

Centre intercommunal d'action sociale
Séance du 13 juin 2018
Délibération n° 13062018D06

VU le code de l'action sociale et des familles ;

VU le code général des collectivités territoriales ;

VU le code des relations entre le public et l'administration ;

VU le code de la propriété intellectuelle ;

VU le code pénal, notamment ses articles 323-1 à 323-8 ;

VU le code civil, notamment ses articles 1316-1 et 1367 ;

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

VU la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;

VU la loi n° 84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale ;

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

VU le décret n° 89-677 du 18 septembre 1989 relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux ;

VU le décret n° 2015-1912 du 29 décembre 2015 portant diverses dispositions relatives aux agents contractuels de la fonction publique territoriale modifiant le décret n° 88-145 du 15 février 1988 relatif aux agents non titulaires de la fonction publique territoriale ;

CONSIDÉRANT la nécessité de formaliser les règles légales et de sécurité relatives à l'utilisation du système d'information et de communication au sein de la Communauté de communes et du Centre intercommunal d'action sociale Maremne Adour Côte-Sud ;

CONSIDÉRANT qu'il y a lieu d'informer les agents de la Communauté de communes et du Centre intercommunal d'action sociale Maremne Adour Côte-Sud sur leurs droits et obligations dans l'utilisation des moyens et outils technologiques de l'information et de la communication ;

CONSIDÉRANT que la charte d'utilisation, telle que proposée en annexe de la présente, sera applicable aux administrateurs bénéficiaires d'une mise à disposition, à titre individuel, de moyens informatiques et de télécommunications nécessaires à l'exercice de leurs mandats ;

décide, après en avoir délibéré et à l'unanimité :

- d'approuver les projets de chartes d'utilisation des moyens et outils technologiques de l'information et de la communication, tels qu'annexés à la présente,

- d'autoriser Monsieur le Président à signer les projets de chartes d'utilisation des moyens et outils technologiques de l'information et de la communication, tels qu'annexés à la présente,

- d'autoriser Monsieur le Président ou son représentant à prendre tout acte et à signer tout document se rapportant à l'exécution de la présente.

La présente délibération pourra faire l'objet d'un recours pour excès de pouvoir dans un délai de deux mois devant le Tribunal administratif de Pau à compter de sa publication ou de son affichage et de sa transmission au représentant de l'État dans le département.

Fait et délibéré les jours, mois et an ci-dessus
Pour extrait certifié conforme
À Saint-Vincent de Tyrosse, le 14 juin 2018

Pour le président,
par délégation
La vice-présidente,

CENTRE INTERCOMMUNAL D'ACTION SOCIALE * MACS *

Frédérique Charpenel

Envoyé en préfecture le 25/06/2018
Reçu en préfecture le 25/06/2018

ID : 040-200009868-20180613-13062018D06-DE

MACS
Communauté de communes
Maremne Adour Côte-Sud

MACS
Centre Intercommunal d'Action Sociale
Maremne Adour Côte-Sud

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

SOMMAIRE

1 - INTRODUCTION 3
1.1 - Le contexte et les enjeux 3
1.2 - L'objectif 3
1.3 - Le champ d'application 3
2 - LES RÈGLES GÉNÉRALES D'UTILISATION 3
2.1 - Les droits et les devoirs des utilisateurs 4
2.1.1 - Un accès aux ressources réglementé 4
2.1.2 - Confidentialité des données produites par l'établissement 4
2.2 - Les droits et les devoirs de l'Établissement 4
2.3 - Les sanctions 5
2.4 - Les Évolutions 5
3 - L'INTERNET 5
4 - LA MESSAGERIE 5
5 - RÉCÉPISSÉ CHARTE D'UTILISATION DES MOTIC 7
6 - ANNEXE 1 - LES BASES LÉGALES 8
7 - ANNEXE 2 - LA NORME SIMPLIFIEE CNIL NS-46 10

1 - INTRODUCTION

1.1 - LE CONTEXTE ET LES ENJEUX

Les différents outils technologiques mis à disposition des élus des collectivités territoriales et de leurs groupements offrent 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.

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 formalise 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 et du Centre intercommunal d'action sociale 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 faire l'objet de poursuites pénales.

1.3 - LE CHAMP D'APPLICATION

La présente charte s'applique aux conseillers et administrateurs bénéficiaires d'une mise à disposition de matériels informatiques dans le cadre de l'exercice de leur mandat.

Dès l'entrée en vigueur de la présente charte, chaque conseiller et administrateur 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 d'établissement qu'il se présente sur Internet et doit se porter garant de l'image de l'institution.

2.1 - LES DROITS ET LES DEVOIRS DES UTILISATEURS

2.1.1 - UN ACCÈS AUX RESSOURCES RÉGLEMENTÉ

Toute personne détenant un mandat dans l'établissement dispose d'un droit d'accès au système d'information. Ce droit d'accès est :

- Strictement personnel ;
- Incessible.

Les ressources informatiques mises à disposition constituent un outil nécessaire à l'exercice du mandat. 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, genre 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 »). Une déclaration à la CNIL est obligatoire pour toute création de fichiers contenant des informations nominatives ;
- 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.

2.1.2 - 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 son représentant légal.

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 des fonctions 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.

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.

2.4 - LES ÉVOLUTIONS

Avant son entrée en vigueur, la présente charte a été approuvée par délibération de l'organe délibérant de l'établissement. Elle pourra être complétée ou modifiée selon les mêmes formes.

3 - L'INTERNET

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 responsable légal de l'établissement 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.

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.

4 - LA MESSAGERIE

L'utilisateur veillera à ne pas ouvrir les courriers électroniques (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 à la norme simplifiée CNIL N°46.

L'utilisateur signera tout courriel professionnel.

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

La présente Charte a été approuvée par délibérations du conseil communautaire du ..... et du conseil d'administration du CIAS du .....

Pour MACS,	Pour le CIAS,
Le président,	La vice-présidente,
Pierre Froustey	Frédérique Charpenel

5 - RÉCÉPISSÉ CHARTE D'UTILISATION DES MOTIC

Je soussigné(e) :

Nom : .....

Prénom : .....

Commune : .....

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.*

6 - ANNEXE 1 - LES BASES LÉGALES

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 REFERENCE

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)

B - LE CODE PENAL

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. »

7 - ANNEXE 2 - La Norme Simplifiée CNIL NS-46

La Commission nationale de l'informatique et des libertés,

Vu la convention n°108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code du travail ;

Vu les lois n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, n°84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat, n°84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale, et n°86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière ;

Vu la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, et notamment ses articles 24 et 69 alinéa 8 ;

Après avoir entendu M. Hubert Bouchet, commissaire, en son rapport et Mme Catherine Pozzo di Borgo, commissaire adjoint du Gouvernement, en ses observations ;

En vertu de l'article 24 de la loi du 6 janvier 1978 modifiée, la Commission nationale de l'informatique et des libertés est habilitée à établir des normes destinées à simplifier l'obligation de déclaration des traitements les plus courants et dont la mise en œuvre, dans des conditions régulières, n'est pas susceptible de porter atteinte à la vie privée ou aux libertés.

Les traitements informatisés relatifs à la gestion de leurs personnels mis en œuvre par des employeurs publics ou privés sont de ceux qui peuvent, sous certaines conditions, relever de cette définition.

Après avoir recueilli les observations des représentants des organisations professionnelles d'employeurs et d'employés, et des ministères concernés,

Décide :

Article 1 :

Peut bénéficier de la procédure de la déclaration simplifiée de conformité à la présente norme tout traitement automatisé relatif à la gestion du personnel des organismes publics ou privés qui répondent aux conditions suivantes.

Article 2 : finalités du traitement

Le traitement peut avoir tout ou partie des finalités suivantes :

La gestion administrative des personnels :

- gestion du dossier professionnel des employés, tenu conformément aux dispositions législatives et réglementaires, ainsi qu'aux dispositions statutaires, conventionnelles ou contractuelles qui régissent les intéressés ;
- réalisation d'états statistiques ou de listes d'employés pour répondre à des besoins de gestion administrative ;
- gestion des annuaires internes et des organigrammes ;
- gestion des dotations individuelles en fournitures, équipements, véhicules et cartes de paiement ;
- gestion des élections professionnelles (*délibération n°2005-277 du 17 novembre 2005*) à l'exclusion du cas où est utilisé un dispositif de vote électronique;
- gestion des réunions des instances représentatives du personnel ;
- gestion de l'action sociale et culturelle directement mise en œuvre par l'employeur, à l'exclusion des activités de médecine du travail, de service social ou de soutien psychologique ;

La mise à disposition des personnels d'outils informatiques :

- suivi et maintenance du parc informatique ;
- gestion des annuaires informatiques permettant de définir les autorisations d'accès aux applications et aux réseaux ;
- mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés ;
- gestion de la messagerie électronique professionnelle, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés ;
- réseaux privés virtuels internes à l'organisme permettant la diffusion ou la collecte de données de gestion administrative des personnels (intranet) ;

L'organisation du travail :

- gestion des agendas professionnels ;
- gestion des tâches des personnels, à l'exclusion de tout traitement permettant un contrôle individuel de leur productivité.

La gestion des carrières et de la mobilité :

- évaluation professionnelle des personnels, dans le respect des dispositions législatives, réglementaires ou conventionnelles qui la régissent, à l'exclusion des dispositifs ayant pour objet l'établissement du profil psychologique des employés ;
- gestion des compétences professionnelles internes ;
- validation des acquis de l'expérience professionnelle ;
- simulation de carrière ;
- gestion de la mobilité professionnelle.

La formation des personnels :

- suivi des demandes de formation et des périodes de formation effectuées ;
- organisation des sessions de formation ;
- évaluation des connaissances et des formations.

Les fonctionnalités de gestion informatisée des courriers et d'archivage électronique des documents produits dans le cadre des finalités précédemment décrites sont couvertes par la présente norme.

Article 3 : données traitées

Les données traitées pour la réalisation des finalités décrites à l'article 2 sont :

a) pour l'identification de l'employé :

- identité : nom, prénom, photographie (facultatif), sexe, date et lieu de naissance, nationalité, coordonnées professionnelles, coordonnées personnelles (facultatif), matricule interne, références du passeport (uniquement pour les personnels amenés à se déplacer à l'étranger) ;
- type, numéro d'ordre et copie du titre valant autorisation de travail pour les employés étrangers en application de l'article R.620-3 du code du travail ;
- le cas échéant, coordonnées des personnes à prévenir en cas d'urgence ;
- distinctions honorifiques (facultatif).

b) pour la gestion administrative de l'employé :

- **gestion de la carrière de l'employé :** date et conditions d'embauche ou de recrutement, date, objet et motif des modifications apportées à la situation professionnelle de l'employé, simulation de carrière, desiderata de l'employé en termes d'emploi, sanctions disciplinaires à l'exclusion de celles consécutives à des faits amnistiés ;
- **gestion des déclarations d'accident du travail et de maladie professionnelle :** coordonnées du médecin du travail, date de l'accident ou de la première constatation médicale de la maladie professionnelle, date du dernier jour de travail, date de reprise, motif de l'arrêt (accident du travail ou maladie professionnelle), travail non repris à ce jour ;
- **évaluation professionnelle de l'employé :** dates des entretiens d'évaluation, identité de l'évaluateur, compétences professionnelles de l'employé, objectifs assignés, résultats obtenus, appréciation des aptitudes professionnelles sur la base de critères objectifs et présentant un lien direct et nécessaire avec l'emploi occupé, observations et souhaits formulés par l'employé, prévisions d'évolution de carrière ;
- **validation des acquis de l'expérience :** date de la demande de validation, diplôme, titre ou certificat de qualification concerné, expériences professionnelles soumises à validation, validation (oui/non), date de la décision ;
- **formation :** diplômes, certificats et attestations, langues étrangères pratiquées, suivi des demandes de formation professionnelle et des périodes de formation effectuées, organisation des sessions de formation, évaluation des connaissances et des formations ;
- **suivi administratif des visites médicales des employés :** dates des visites, aptitude au poste de travail (apte ou inapte, propositions d'adaptation du poste de travail ou d'affectation à un autre poste de travail formulées par le médecin du travail) ;
- **type de permis de conduire détenu par l'employé ;**
- **sujétions particulières ouvrant droit à congés spéciaux ou à un crédit d'heures de délégation** (telles que l'exercice d'un mandat électif ou représentatif syndical, la participation à la réserve opérationnelle ou aux missions de sapeur-pompier volontaire) ;

c) pour l'organisation du travail :

- **annuaires internes et organigrammes** : nom, prénom, photographie (facultatif), fonction, coordonnées professionnelles, le cas échéant, formation et réalisations professionnelles ;
- **agendas professionnels :** dates, lieux et heures des rendez-vous professionnels, objet, personnes présentes ;
- **tâches des personnels :** identification des personnels concernés, répartition des tâches ;
- **gestion des dotations individuelles en fournitures, équipements, véhicules et cartes de paiement** : gestion des demandes, nature de la dotation, dates de dotation, de maintenance et de retrait, affectations budgétaires ;
- **annuaires informatiques permettant de définir les autorisations d'accès aux applications et aux réseaux** ;
- **données de connexion enregistrées pour assurer la sécurité et le bon fonctionnement des applications et des réseaux informatiques, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés** ;

- **messagerie électronique** : carnet d'adresses, comptes individuels, à l'exclusion de toute donnée relative au contrôle individuel des communications électroniques émises ou reçues par les employés ;
- **réseaux privés virtuels de diffusion ou de collecte de données de gestion administrative des personnels (intranet)** : formulaires administratifs internes, organigrammes, espaces de discussion, espaces d'information.

d) pour l'action sociale et la représentation du personnel :

- **gestion des activités sociales et culturelles mises en œuvre par l'employeur :** identité de l'employé et de ses ayants droit ou ouvrants droit, revenus, avantages et prestations demandés et servis ;
- **élections professionnelles** : établissement de la liste électorale (identité des électeurs, âge, ancienneté, collège), gestion des candidatures (identité, nature du mandat sollicité, éléments permettant de vérifier le respect des conditions d'éligibilité, le cas échéant appartenance syndicale déclarée par les candidats) et publication des résultats (identité des candidats, mandats concernés, nombre et pourcentage de suffrages obtenus, identité des personnels élus et, le cas échéant, appartenance syndicale des élus) ;
- **gestion des réunions des instances représentatives du personnel** : convocations, documents préparatoires, procès-verbaux.

Article 4 : personnes concernées

Sont concernées par le traitement les personnes employées par des organismes publics ou privés, quelle que soit la nature de leur emploi.

Article 5 : destinataires des données

Dans le respect des textes applicables, seules les données visées à l'article 3 strictement nécessaires à l'accomplissement de leurs missions sont communiquées aux destinataires suivants :

- **les personnes habilitées chargées de la gestion du personnel** ;
- **les supérieurs hiérarchiques des employés concernés, à l'exclusion des données relatives à l'action sociale directement mise en œuvre par l'employeur** ;
- **les instances représentatives du personnel** : après recueil de l'accord exprès des intéressés, coordonnées professionnelles des employés et données strictement nécessaires à leur représentation ;
- **les délégués syndicaux** : coordonnées professionnelles des employés après accord formalisé avec l'employeur et recueil de l'accord exprès des intéressés, et données strictement nécessaires à la défense des intérêts des employés.

Ces destinataires assurent la stricte confidentialité des données personnelles en leur possession.

Article 6 : durée de conservation

Les données visées à l'article 3 ne sont pas conservées par les services gestionnaires au-delà de la période d'emploi de la personne concernée, sans préjudice de dispositions législatives ou réglementaires propres à certaines catégories de données imposant une durée de conservation particulière ou la suppression de ces données.

Les données relatives aux sujétions particulières ouvrant droit à congés spéciaux ou à un crédit d'heures de délégation ne sont pas conservées au-delà de la période de sujétion de l'employé concerné.

Au-delà, ces données peuvent être archivées sur un support informatique distinct et à accès très limité, conformément aux règles applicables en matière d'archives publiques et d'archives privées.

Article 7 : information des personnes concernées

Les personnes concernées sont informées de l'identité du responsable du traitement, des finalités poursuivies, du caractère obligatoire ou facultatif des réponses à apporter, des conséquences éventuelles, à leur égard, d'un défaut de réponse, des destinataires des données, (*délibération n°2005-277 du 17 novembre 2005*) le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un état non membre de l'Union européenne et de leurs droits d'opposition, pour des motifs légitimes, au traitement de leurs données sauf dans les cas où le traitement répond à une obligation légale, d'accès aux données les concernant et de rectification de ces données.

Cette information est délivrée à tout employé par la remise d'un document écrit ou par voie électronique.

Le responsable du traitement procède également, conformément aux dispositions du code du travail et à la législation applicable aux trois fonctions publiques, à l'information et à la consultation des instances représentatives du personnel avant la mise en œuvre des traitements visés à l'article 2.

Article 8 : sécurités

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité des données visées à l'article 3 et, notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

En particulier, des mesures permettant de contrôler les accès au traitement et de sécuriser les communications des données sont mises en œuvre.

Article 9 : transfert de données vers l'étranger

(délibération n° 2005-277 du 17 novembre 2005)

Certains transferts de données à caractère personnel peuvent être réalisés vers des pays tiers à l'Union européenne qui ne sont pas membres de l'Espace économique européen et qui n'ont pas été reconnus par une décision de la Commission européenne comme assurant un niveau de protection adéquat, dès lors que :

le traitement garantit un niveau suffisant de protection de la vie privée ainsi que des droits et libertés fondamentaux des personnes en raison de la mise en œuvre des clauses contractuelles types émises par la Commission européenne dans ses décisions du 15 juin 2001 (décision n°2001/497/CE), du 27 décembre 2001 (décision n°2002/16/CE) ou du 27 décembre 2004 (décision n°2004/915/CE) ou par l'adoption de règles internes d'entreprise ayant fait l'objet d'une décision favorable de la Commission nationale de l'informatique et des libertés ;

Le responsable de traitement a clairement informé les personnes de l'existence d'un transfert de données vers des pays tiers conformément aux dispositions de l'article 32 de la loi informatique et libertés et de l'article 7 de la présente norme ;

Le responsable de traitement s'engage, sur simple demande de la personne concernée, à apporter une information complète sur : la finalité du transfert, les données transférées, les destinataires exacts des informations et les moyens mis en œuvre pour encadrer ce transfert.

Peuvent seuls faire l'objet d'un transfert de données vers certains pays situés en dehors de l'Union européenne (dès lors qu'ils ne permettent pas un contrôle de l'activité individuelle des agents), les traitements ayant pour finalité :

La gestion administrative des personnels mais uniquement pour les traitements permettant :

- la réalisation d'états statistiques ou de listes d'employés pour répondre à des besoins de gestion administrative

- la gestion des annuaires internes et des organigrammes ;
- la mise à disposition des personnels d'outils informatiques :
- suivi et maintenance du parc informatique ;
- gestion des annuaires informatiques permettant de définir les autorisations d'accès aux applications et aux réseaux ;
- mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés ;
- gestion de la messagerie électronique professionnelle, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés ;
- réseaux privés virtuels internes à l'organisme permettant la diffusion ou la collecte de données de gestion administrative des personnels (intranet) ;

Pour chacune de ces finalités, les données pouvant être transférées sont celles limitativement prévues par l'article 3 de la présente norme.

Article 10 : exclusion du bénéfice de la norme simplifiée

Tout traitement non conforme aux dispositions des articles 2 à 9 de la présente décision ne peut faire l'objet d'une déclaration simplifiée auprès de la CNIL en référence à la présente norme.

Article 11 :

La norme simplifiée n°37 établie par délibération n°93-021 du 2 mars 1993 est abrogée.

Article 12 :

La présente délibération est publiée au Journal officiel de la République française.

Envoyé en préfecture le 25/06/2018
Reçu en préfecture le 25/06/2018
ID : 040-200009868-20180613-13062018D06-DE

MACS
Communauté de communes
Maremne Adour Côte-Sud

MACS
Centre Intercommunal d'Action Sociale
Maremne Adour Côte-Sud

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

SOMMAIRE

1 - INTRODUCTION 3
1.1 - Le contexte et les enjeux 3
1.2 - L'objectif 3
1.3 - Le champ d'application 3
2 - LES RÈGLES GÉNÉRALES D'UTILISATION 4
2.1 - Les droits et les devoirs des utilisateurs 4
2.1.1 - UN ACCÉS AUX RESSOURCES RÉGLEMENTÉ 4
2.1.2 - UNE UTILISATION PROFESSIONNELLE DES RESSOURCES 4
2.1.3 - CONFIDENTIALITÉ DES DONNÉES PRODUITES PAR L'ÉTABLISSEMENT 5
2.2 - Les droits et les devoirs de l'Établissement 5
2.3 - Les sanctions 5
2.4 - Les Évolutions 6
3 - LES POSTES INFORMATIQUES 6
4 - LA MESSAGERIE 7
4.1 - Règles d'utilisation 7
5 - L'INTERNET 8
5.1 - Règles d'utilisation 8
6 - LE TÉLÉPHONE 9
6.1 - Règles d'utilisation 9
7 - DROIT À LA DÉCONNEXION DES AGENTS 9
7.1 - Des actions d'information et de formation 10
7.2 - Des actions de prévention des risques professionnels (chsct) 10
8 - GLOSSAIRE 11
9 - RÉCÉPISSÉ CHARTE D'UTILISATION DES MOTIC 12
10 - ANNEXE 1 - LES BASES LÉGALES 13
11 - ANNEXE 2 - La Norme Simplifiée CNIL NS-46 15
12 - ANNEXE 3 - La Norme Simplifiée CNIL NS-47 21

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 et du Centre intercommunal d'action sociale 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. 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 d'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 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, genre 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 »). Une déclaration à la CNIL est obligatoire pour toute création de fichiers contenant des informations nominatives ;
- 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 - 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.

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 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, etc.) ;
- 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).

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 - LA MESSAGERIE

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

4.1 - 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.

La lecture des courriers électroniques (courriels) personnels reçus durant les heures de travail est tolérée, si celle-ci reste occasionnelle.

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 à la norme simplifiée CNIL N°46.

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.

5 - L'INTERNET

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

5.1 - 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 à la norme simplifiée CNIL N°46.

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.

6 - LE TÉLÉPHONE

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

6.1 - 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 respectant les conditions prévues dans la norme CNIL simplifiée N° 47.

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.

7 - 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 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 :

7.1 - 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.

7.2 - 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.

La présente Charte a été approuvée par délibérations du conseil communautaire du ..... et du conseil d'administration du CIAS du .....

Pour MACS,	Pour le CIAS,
Le président,	La vice-présidente,
Pierre Froustey	Frédérique Charpenel

8 - 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)

9 - 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.*

10 - 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 REFERENCE

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 PENAL

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. »

11 - ANNEXE 2 - La Norme Simplifiée CNIL NS-46

La Commission nationale de l'informatique et des libertés,

Vu la convention n°108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code du travail ;

Vu les lois n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, n°84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat, n°84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale, et n°86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière ;

Vu la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, et notamment ses articles 24 et 69 alinéa 8 ;

Après avoir entendu M. Hubert Bouchet, commissaire, en son rapport et Mme Catherine Pozzo di Borgo, commissaire adjoint du Gouvernement, en ses observations ;

En vertu de l'article 24 de la loi du 6 janvier 1978 modifiée, la Commission nationale de l'informatique et des libertés est habilitée à établir des normes destinées à simplifier l'obligation de déclaration des traitements les plus courants et dont la mise en œuvre, dans des conditions régulières, n'est pas susceptible de porter atteinte à la vie privée ou aux libertés.

Les traitements informatisés relatifs à la gestion de leurs personnels mis en œuvre par des employeurs publics ou privés sont de ceux qui peuvent, sous certaines conditions, relever de cette définition.

Après avoir recueilli les observations des représentants des organisations professionnelles d'employeurs et d'employés, et des ministères concernés,

Décide :

Article 1 :

Peut bénéficier de la procédure de la déclaration simplifiée de conformité à la présente norme tout traitement automatisé relatif à la gestion du personnel des organismes publics ou privés qui répondent aux conditions suivantes.

Article 2 : finalités du traitement

Le traitement peut avoir tout ou partie des finalités suivantes :

La gestion administrative des personnels :

- gestion du dossier professionnel des employés, tenu conformément aux dispositions législatives et réglementaires, ainsi qu'aux dispositions statutaires, conventionnelles ou contractuelles qui régissent les intéressés ;
- réalisation d'états statistiques ou de listes d'employés pour répondre à des besoins de gestion administrative ;
- gestion des annuaires internes et des organigrammes ;
- gestion des dotations individuelles en fournitures, équipements, véhicules et cartes de paiement ;
- gestion des élections professionnelles (*délibération n°2005-277 du 17 novembre 2005*) à l'exclusion du cas où est utilisé un dispositif de vote électronique;
- gestion des réunions des instances représentatives du personnel ;
- gestion de l'action sociale et culturelle directement mise en œuvre par l'employeur, à l'exclusion des activités de médecine du travail, de service social ou de soutien psychologique ;

La mise à disposition des personnels d'outils informatiques :

- suivi et maintenance du parc informatique ;
- gestion des annuaires informatiques permettant de définir les autorisations d'accès aux applications et aux réseaux ;
- mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés ;
- gestion de la messagerie électronique professionnelle, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés ;
- réseaux privés virtuels internes à l'organisme permettant la diffusion ou la collecte de données de gestion administrative des personnels (intranet) ;

L'organisation du travail :

- gestion des agendas professionnels ;
- gestion des tâches des personnels, à l'exclusion de tout traitement permettant un contrôle individuel de leur productivité.

La gestion des carrières et de la mobilité :

- évaluation professionnelle des personnels, dans le respect des dispositions législatives, réglementaires ou conventionnelles qui la régissent, à l'exclusion des dispositifs ayant pour objet l'établissement du profil psychologique des employés ;
- gestion des compétences professionnelles internes ;
- validation des acquis de l'expérience professionnelle ;
- simulation de carrière ;
- gestion de la mobilité professionnelle.

La formation des personnels :

- suivi des demandes de formation et des périodes de formation effectuées ;
- organisation des sessions de formation ;
- évaluation des connaissances et des formations.

Les fonctionnalités de gestion informatisée des courriers et d'archivage électronique des documents produits dans le cadre des finalités précédemment décrites sont couvertes par la présente norme.

Article 3 : données traitées

Les données traitées pour la réalisation des finalités décrites à l'article 2 sont :

a) pour l'identification de l'employé :

- identité : nom, prénom, photographie (facultatif), sexe, date et lieu de naissance, nationalité, coordonnées professionnelles, coordonnées personnelles (facultatif), matricule interne, références du passeport (uniquement pour les personnels amenés à se déplacer à l'étranger) ;
- type, numéro d'ordre et copie du titre valant autorisation de travail pour les employés étrangers en application de l'article R.620-3 du code du travail ;
- le cas échéant, coordonnées des personnes à prévenir en cas d'urgence ;
- distinctions honorifiques (facultatif).

b) pour la gestion administrative de l'employé :

- **gestion de la carrière de l'employé :** date et conditions d'embauche ou de recrutement, date, objet et motif des modifications apportées à la situation professionnelle de l'employé, simulation de carrière, desiderata de l'employé en termes d'emploi, sanctions disciplinaires à l'exclusion de celles consécutives à des faits amnistiés ;
- **gestion des déclarations d'accident du travail et de maladie professionnelle :** coordonnées du médecin du travail, date de l'accident ou de la première constatation médicale de la maladie professionnelle, date du dernier jour de travail, date de reprise, motif de l'arrêt (accident du travail ou maladie professionnelle), travail non repris à ce jour ;
- **évaluation professionnelle de l'employé :** dates des entretiens d'évaluation, identité de l'évaluateur, compétences professionnelles de l'employé, objectifs assignés, résultats obtenus, appréciation des aptitudes professionnelles sur la base de critères objectifs et présentant un lien direct et nécessaire avec l'emploi occupé, observations et souhaits formulés par l'employé, prévisions d'évolution de carrière ;
- **validation des acquis de l'expérience :** date de la demande de validation, diplôme, titre ou certificat de qualification concerné, expériences professionnelles soumises à validation, validation (oui/non), date de la décision ;
- **formation :** diplômes, certificats et attestations, langues étrangères pratiquées, suivi des demandes de formation professionnelle et des périodes de formation effectuées, organisation des sessions de formation, évaluation des connaissances et des formations ;
- **suivi administratif des visites médicales des employés :** dates des visites, aptitude au poste de travail (apte ou inapte, propositions d'adaptation du poste de travail ou d'affectation à un autre poste de travail formulées par le médecin du travail) ;
- **type de permis de conduire détenu par l'employé ;**
- **sujétions particulières ouvrant droit à congés spéciaux ou à un crédit d'heures de délégation** (telles que l'exercice d'un mandat électif ou représentatif syndical, la participation à la réserve opérationnelle ou aux missions de sapeur-pompier volontaire) ;

c) pour l'organisation du travail :

- **annuaires internes et organigrammes** : nom, prénom, photographie (facultatif), fonction, coordonnées professionnelles, le cas échéant, formation et réalisations professionnelles ;
- **agendas professionnels :** dates, lieux et heures des rendez-vous professionnels, objet, personnes présentes ;
- **tâches des personnels :** identification des personnels concernés, répartition des tâches ;

- **gestion des dotations individuelles en fournitures, équipements, véhicules et cartes de paiement** : gestion des demandes, nature de la dotation, dates de dotation, de maintenance et de retrait, affectations budgétaires ;
- **annuaires informatiques permettant de définir les autorisations d'accès aux applications et aux réseaux** ;
- **données de connexion enregistrées pour assurer la sécurité et le bon fonctionnement des applications et des réseaux informatiques, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés** ;
- **messagerie électronique** : carnet d'adresses, comptes individuels, à l'exclusion de toute donnée relative au contrôle individuel des communications électroniques émises ou reçues par les employés ;
- **réseaux privés virtuels de diffusion ou de collecte de données de gestion administrative des personnels (intranet)** : formulaires administratifs internes, organigrammes, espaces de discussion, espaces d'information.

d) pour l'action sociale et la représentation du personnel :

- **gestion des activités sociales et culturelles mises en œuvre par l'employeur :** identité de l'employé et de ses ayants droit ou ouvrants droit, revenus, avantages et prestations demandés et servis ;
- **élections professionnelles** : établissement de la liste électorale (identité des électeurs, âge, ancienneté, collège), gestion des candidatures (identité, nature du mandat sollicité, éléments permettant de vérifier le respect des conditions d'éligibilité, le cas échéant appartenance syndicale déclarée par les candidats) et publication des résultats (identité des candidats, mandats concernés, nombre et pourcentage de suffrages obtenus, identité des personnels élus et, le cas échéant, appartenance syndicale des élus) ;
- **gestion des réunions des instances représentatives du personnel** : convocations, documents préparatoires, procès-verbaux.

Article 4 : personnes concernées

Sont concernées par le traitement les personnes employées par des organismes publics ou privés, quelle que soit la nature de leur emploi.

Article 5 : destinataires des données

Dans le respect des textes applicables, seules les données visées à l'article 3 strictement nécessaires à l'accomplissement de leurs missions sont communiquées aux destinataires suivants :

- **les personnes habilitées chargées de la gestion du personnel** ;
- **les supérieurs hiérarchiques des employés concernés, à l'exclusion des données relatives à l'action sociale directement mise en œuvre par l'employeur** ;
- **les instances représentatives du personnel** : après recueil de l'accord exprès des intéressés, coordonnées professionnelles des employés et données strictement nécessaires à leur représentation ;
- **les délégués syndicaux** : coordonnées professionnelles des employés après accord formalisé avec l'employeur et recueil de l'accord exprès des intéressés, et données strictement nécessaires à la défense des intérêts des employés.

Ces destinataires assurent la stricte confidentialité des données personnelles en leur possession.

Article 6 : durée de conservation

Les données visées à l'article 3 ne sont pas conservées par les services gestionnaires au-delà de la période d'emploi de la personne concernée, sans préjudice de dispositions législatives ou réglementaires propres à certaines catégories de données imposant une durée de conservation particulière ou la suppression de ces données.

Les données relatives aux sujétions particulières ouvrant droit à congés spéciaux ou à un crédit d'heures de délégation ne sont pas conservées au-delà de la période de sujétion de l'employé concerné.

Au-delà, ces données peuvent être archivées sur un support informatique distinct et à accès très limité, conformément aux règles applicables en matière d'archives publiques et d'archives privées.

Article 7 : information des personnes concernées

Les personnes concernées sont informées de l'identité du responsable du traitement, des finalités poursuivies, du caractère obligatoire ou facultatif des réponses à apporter, des conséquences éventuelles, à leur égard, d'un défaut de réponse, des destinataires des données, (*délibération n°2005-277 du 17 novembre 2005*) le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un état non membre de l'Union européenne et de leurs droits d'opposition, pour des motifs légitimes, au traitement de leurs données sauf dans les cas où le traitement répond à une obligation légale, d'accès aux données les concernant et de rectification de ces données.

Cette information est délivrée à tout employé par la remise d'un document écrit ou par voie électronique.

Le responsable du traitement procède également, conformément aux dispositions du code du travail et à la législation applicable aux trois fonctions publiques, à l'information et à la consultation des instances représentatives du personnel avant la mise en œuvre des traitements visés à l'article 2.

Article 8 : sécurités

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité des données visées à l'article 3 et, notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

En particulier, des mesures permettant de contrôler les accès au traitement et de sécuriser les communications des données sont mises en œuvre.

Article 9 : transfert de données vers l'étranger

(délibération n° 2005-277 du 17 novembre 2005)

Certains transferts de données à caractère personnel peuvent être réalisés vers des pays tiers à l'Union européenne qui ne sont pas membres de l'Espace économique européen et qui n'ont pas été reconnus par une décision de la Commission européenne comme assurant un niveau de protection adéquat, dès lors que :

le traitement garantit un niveau suffisant de protection de la vie privée ainsi que des droits et libertés fondamentaux des personnes en raison de la mise en œuvre des clauses contractuelles types émises par la Commission européenne dans ses décisions du 15 juin 2001 (décision n°2001/497/CE), du 27 décembre 2001 (décision n°2002/16/CE) ou du 27 décembre 2004 (décision n°2004/915/CE) ou par l'adoption de règles internes d'entreprise ayant fait l'objet d'une décision favorable de la Commission nationale de l'informatique et des libertés ;

Le responsable de traitement a clairement informé les personnes de l'existence d'un transfert de données vers des pays tiers conformément aux dispositions de l'article 32 de la loi informatique et libertés et de l'article 7 de la présente norme ;

Le responsable de traitement s'engage, sur simple demande de la personne concernée, à apporter une information complète sur : la finalité du transfert, les données transférées, les destinataires exacts des informations et les moyens mis en œuvre pour encadrer ce transfert.

Peuvent seuls faire l'objet d'un transfert de données vers certains pays situés en dehors de l'Union européenne (dès lors qu'ils ne permettent pas un contrôle de l'activité individuelle des agents), les traitements ayant pour finalité :

La gestion administrative des personnels mais uniquement pour les traitements permettant :

- la réalisation d'états statistiques ou de listes d'employés pour répondre à des besoins de gestion administrative
- la gestion des annuaires internes et des organigrammes ;
- la mise à disposition des personnels d'outils informatiques :
- suivi et maintenance du parc informatique ;
- gestion des annuaires informatiques permettant de définir les autorisations d'accès aux applications et aux réseaux ;
- mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés ;
- gestion de la messagerie électronique professionnelle, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés ;
- réseaux privés virtuels internes à l'organisme permettant la diffusion ou la collecte de données de gestion administrative des personnels (intranet) ;

Pour chacune de ces finalités, les données pouvant être transférées sont celles limitativement prévues par l'article 3 de la présente norme.

Article 10 : exclusion du bénéfice de la norme simplifiée

Tout traitement non conforme aux dispositions des articles 2 à 9 de la présente décision ne peut faire l'objet d'une déclaration simplifiée auprès de la CNIL en référence à la présente norme.

Article 11 :

La norme simplifiée n°37 établie par délibération n°93-021 du 2 mars 1993 est abrogée.

Article 12 :

La présente délibération est publiée au Journal officiel de la République française.

12 - ANNEXE 3 - La Norme Simplifiée CNIL NS-47

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/47/CE du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu les lois n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, n°84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat, n° 84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale, et n° 86-33 du 9 janvier 1986 portant dispositions statutaires à la fonction publique hospitalière ;

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

Vu le code des postes et des communications électroniques ;

Vu le code du travail ;

Vu l'arrêté du 1er février 2002 relatif aux factures des services téléphoniques ;

Vu la délibération de la CNIL n°94-113 du 20 décembre 1994 portant adoption d'une norme simplifiée concernant les traitements automatisés d'informations nominatives mis en œuvre à l'aide d'autocommutateurs téléphoniques sur les lieux de travail (norme simplifiée n°40) ;

Après avoir entendu M. Didier Gasse, commissaire, en son rapport et Mme Catherine Pozzo di Borgo, commissaire adjoint du Gouvernement, en ses observations ;

Formule les observations suivantes :

En application des articles 11 et 24-I. de la loi du 6 janvier 1978 modifiée, la CNIL est habilitée à édicter des normes simplifiées concernant certains traitements automatisés de données à caractère personnel.

Pour l'application de l'article 24-I. susvisé, il faut entendre par norme simplifiée un texte à valeur réglementaire définissant l'ensemble des conditions que doit remplir une catégorie courante de traitements pour être regardée comme ne comportant manifestement pas de risques d'atteinte à la vie privée et aux libertés et comme pouvant, dès lors, faire l'objet d'une déclaration simplifiée de conformité.

La mise à disposition au bénéfice des employés d'une ligne téléphonique, fixe ou mobile, conduit l'employeur public ou privé à disposer des données relatives à l'utilisation de ce moyen de communication, que ces données soient issues de la mise en place d'un autocommutateur téléphonique (téléphonie fixe) ou de leur transmission par l'opérateur auprès duquel l'organisme est client (téléphonie fixe ou mobile).

L'utilisation d'un service de téléphonie mobile par les employés d'un organisme public ou privé peut conduire celui-ci à traiter informatiquement les données issues de l'utilisation de ces services, que ces données soient ressaisies par l'entreprise ou l'organisme privé et public à partir des factures papier envoyées par l'opérateur,

qu'elles soient transférées par voie électronique par l'opérateur ou encore qu'elles soient accessibles à l'organisme par l'intermédiaire du site web de l'opérateur.

Les dispositions du code des postes et des communications électroniques permettent aux clients d'un opérateur de recevoir une facturation détaillée qui n'indique pas les quatre derniers chiffres des numéros appelés, à moins que le client n'ait expressément demandé que cela soit le cas. Dès lors, une entreprise ou un organisme privé et public peut avoir accès, soit par l'intermédiaire de l'autocommutateur qu'il aura mis en place, soit par l'intermédiaire de l'opérateur auprès duquel il est client, à l'intégralité des numéros de téléphone appelés.

Si les autocommutateurs permettent la collecte systématique, et à son insu, des données relatives à l'identification de l'appelant, une telle collecte est contraire à l'article 6 de la loi du 6 janvier 1978 modifiée qui prévoit que les données sont collectées et traitées de manière loyale et licite.

Les traitements mis en œuvre dans le cadre de l'utilisation des services de téléphonie ne doivent pas entraver l'exercice des droits reconnus par la loi en matière de droits et libertés des employés protégés.

La mise à disposition de services de communications téléphoniques au sein d'une entreprise ou d'un organisme privé et public est essentiellement destinée à satisfaire les besoins de fonctionnement de l'organisme mais, toutefois, un usage raisonnable par les employés à des fins privées de ces moyens de communication est admis.

Les numéros de téléphone constituent des données à caractère personnel au sens de l'article 2 de la loi du 6 janvier 1978 modifiée ; en conséquence, lorsque les numéros appelés sont enregistrés ou traités dans un fichier informatique, l'opération qui en est ainsi faite constitue un traitement automatisé de données à caractère personnel soumis aux formalités préalables prévues par le chapitre IV de la loi du 6 janvier 1978 modifiée.

Après avoir recueilli les observations des représentants des organisations professionnelles d'employeurs et d'employés, et des ministères concernés :

Décide :

- D'abroger la norme simplifiée n°94-113 du 20 décembre 1994 portant adoption d'une norme simplifiée concernant les traitements automatisés d'informations nominatives mis en œuvre à l'aide d'autocommutateurs téléphoniques sur les lieux de travail (norme simplifiée n°40) ;
- D'adopter une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de l'utilisation de services de téléphonie fixe ou mobile sur les lieux de travail (norme simplifiée n° 47) dont le contenu est le suivant :

Article 1 :

Pour les entreprises ou organismes privés et publics, la déclaration simplifiée effectuée en référence à la présente norme remplace la déclaration simplifiée effectuée en référence à la norme simplifiée 40.

Article 2 : Finalités

Seuls peuvent être déclarés en référence à la présente norme, les traitements mis en œuvre par les entreprises ou organismes privés et publics pour les finalités suivantes :

a) la gestion de la dotation en matériel téléphonique et la maintenance du parc téléphonique ;

b) la gestion de l'annuaire téléphonique interne à savoir, la constitution, l'édition et la diffusion de listes nominatives des utilisateurs des services téléphoniques ;

c) la gestion technique de la messagerie interne de l'organisme ;

d) le remboursement des services de téléphonie utilisés à titre privé par les employés lorsque le caractère privé de l'utilisation de ces services est déterminé par les employés eux-mêmes ;

e) la maîtrise des dépenses liées à l'utilisation professionnelle des services de téléphonie, à savoir l'établissement et l'édition des relevés liés à l'utilisation des services de téléphonie, le calcul du coût de cette utilisation et l'établissement de statistiques anonymes ;

f) la maîtrise des dépenses liées à l'utilisation effectuée à titre privé des services de téléphonie, dans les conditions prévues à l'article 6 de la présente norme.

Les traitements concernés par la présente norme sont exclusifs de tout dispositif permettant l'écoute ou l'enregistrement d'une communication, ou la localisation d'un employé à partir de l'usage de son téléphone mobile.

Article 3 : Informations collectées et traitées

Peuvent seules être collectées et traitées les données suivantes :

a) identité de l'utilisateur du service téléphonique : nom, prénom et numéro de ligne ;

b) situation professionnelle : fonction, service, adresses professionnelles y compris électroniques ;

c) utilisation des services de téléphonie : numéro de téléphone appelé, service utilisé, opérateur appelé, nature de l'appel (sous la forme : local, départemental, national, international), durée, date et heure de début et de fin de l'appel, éléments de facturation (nombre de taxes, volume et nature des données échangées à l'exclusion du contenu de celles-ci et coût du service utilisé).

Lorsque des relevés justificatifs des numéros de téléphone appelés sont établis, les quatre derniers chiffres de ces numéros sont occultés, à l'exception des hypothèses prévues à l'article 6 de la présente norme.

Article 4 : Durée de conservation

Les données à caractère personnel relatives à l'utilisation des services de téléphonie ne peuvent être conservées au-delà du délai prévu à l'article L. 34-2 du code des postes et des communications électroniques, à savoir un an courant à la date de l'exigibilité des sommes dues en paiement des prestations des services de téléphonie.

Article 5 : Destinataires des informations

En fonction des finalités retenues à l'article 2, les destinataires des informations peuvent être :

- pour les données relatives à l'annuaire téléphonique : l'ensemble du personnel ;
- pour les données relatives à la messagerie interne : le titulaire du compte de messagerie concerné ;
- pour les données relatives à la consommation des services téléphoniques : les personnels habilités des services comptables ou financiers chargés de l'élaboration des relevés de communication, les agents disposant du poste téléphonique concerné et, dans les conditions prévues à l'article 6 de la présente norme, les supérieurs hiérarchiques des personnels concernés et les personnels du service du personnel en cas d'utilisation manifestement abusive constatée à l'occasion de l'établissement des relevés non détaillés.
- pour l'ensemble des données : les personnels des services techniques chargés de la mise en œuvre et de la maintenance du service téléphonique dans le strict cadre de leurs attributions ;

Les destinataires assurent la stricte confidentialité des données à caractère personnel en leur possession.

Article 6 : Utilisations des relevés justificatifs complets des numéros de téléphone appelés ou des services de téléphonie utilisés

Une entreprise ou un organisme privé et public peut éditer, soit par l'intermédiaire de l'autocommutateur qu'il aura mis en place, soit par l'intermédiaire de l'opérateur auprès duquel il est client, l'intégralité des numéros de téléphone appelés ou le détail des services de téléphonie utilisés dans les deux cas suivants.

Dans le cas où un remboursement est demandé aux employés pour les services de téléphonie utilisés à titre privé, lorsque le montant demandé est contesté par l'employé auquel il se rapporte, un relevé justificatif complet des données relatives à l'utilisation des services de téléphonie comprenant l'intégralité des numéros de téléphone appelés peut être établi à des fins de preuves.

Dans le cas où l'employeur constate une utilisation manifestement anormale au regard de l'utilisation moyenne constatée au sein de l'entreprise ou de l'organisme privé et public des services de téléphonie, un relevé justificatif complet des numéros de téléphone appelés ou des services de téléphonie utilisés peut être établi de façon contradictoire avec l'employé concerné.

Article 7 : Respect des droits et libertés des employés protégés

Des mesures particulières doivent être prises afin que les conditions de mise en œuvre et d'utilisation des services de téléphonie n'entravent pas l'exercice des droits reconnus par la loi en matière de droits et libertés des représentants des personnels et des employés protégés.

A cet effet, ils doivent pouvoir disposer d'une ligne téléphonique excluant toute possibilité d'interception de leurs communications ou d'identification de leurs correspondants.

Article 8 : Sécurités

Des mesures de sécurité physique et logique doivent être prises afin de préserver la sécurité du traitement et des informations, d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

Article 9 : Information et droit d'accès

L'information des utilisateurs sur les finalités et les fonctions des traitements mis en œuvre, sur les destinataires des informations et sur les modalités d'exercice de leur droit d'accès et de rectification, doit être assurée par tout moyen approprié, notamment par voie d'affichage ou de diffusion de note explicative préalablement à la mise en fonction de ce traitement.

En particulier, lorsque l'entreprise, l'administration ou l'organisme envisage de mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications, dans le respect des dispositions de la présente norme, il doit être procédé à la consultation des instances représentatives du personnel conformément aux textes en vigueur.

Article 10 : Publication au Journal officiel

La présente délibération sera publiée au Journal officiel de la République française.