Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

DEPARTEMENT DES LANDES

COMMUNE DE TARTAS
ARRONDISSEMENT DE DAX

Nombre de Conseillers en exercice : 23
(- 1 démission : Laurine COUFFIGNAL) : 22
Nombre de présents : 13
Nombre de votants : 18
Date de convocation : 05/06/2019

EXTRAIT DU PROCÈS-VERBAL
DES
DÉLIBÉRATIONS DU CONSEIL MUNICIPAL
du Mardi 11 juin 2019
--- o0o ---

L'an deux mille dix-neuf, le onze juin, le Conseil Municipal de la Commune de TARTAS, s'est réuni au lieu ordinaire de ses séances, après convocation légale, sous la présidence de M. BROQUÈRES Jean-François, Maire.

Etaient présents : MM. BROQUÈRES (a procuration pour Mme THIEBLIN), LAMOTHE (a procuration pour Mme BRUGAT), Mme DEGOS, MM. DUBOS (a procuration pour M. GOSSELIN), MARSAN, LAFOURCADE (a procuration pour Mme COURROS), GAILLARDET (a procuration pour M. DUPLA), Mme CHAPUIS, M. DUBUN, Mmes GARRIDO, DAUGREILH, M. DUCASSE, Mme CELIMON.

Etaient excusés : Mmes COURROS (a donné procuration à M. LAFOURCADE), BRUGAT (a donné procuration à M. LAMOTHE), DARGELOSSE, DUBOIS-MAURY, MM. BRUEY, GOSSELIN (a donné procuration à M. DUBOS), DUPLA (a donné procuration à M. GAILLARDET), Mme THIEBLIN (a donné procuration à M. BROQUÈRES).

Etait absent non excusé : M. TAUZIA.

Un scrutin a eu lieu, Mme CELIMON a été élue pour remplir les fonctions de secrétaire.

Séance C
Délibération n°13

DELIBERATION

Rapporteur : M. le Maire

Objet : RGPD – projet de Charte INFORMATIQUE Ville de TARTAS – Services municipaux

M. le Maire présente le projet :
Comme vous le savez la commune de TARTAS a délibéré au premier semestre 2018, sur la démarche RGPD et la désignation du DPO (Délégué aux Protections des Données).
Depuis différentes actions d'information et de sensibilisation ont été menées auprès des Elus municipaux, des services municipaux, et des Chefs de services. Les services de l'ALPI et de l'ADACL ont complété ces actions par des réunions de formation.

Aujourd'hui, afin de mettre en place une charte informatique, qui complète la démarche et précise aussi pour les services Municipaux et Elus les préconisations, méthodes et obligations à suivre, il est proposé :

De soumettre le projet de charte à l'avis du CT de la collectivité.
De l'adapter aux besoins de la commune et de ses missions ou services.
D'indiquer que la charte définitive sera applicable dans le courant du dernier trimestre 2019, après nouvelle délibération du Conseil municipal.

Enfin, il est précisé que la liste de l'ensemble des fichiers tenus et déclarés dans les différents services municipaux, postes informatiques et serveur a été transmise au DPO et à l'ADACL début juin 2019.

.../...

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019

ID : 040-214003139-20190611-2019_C13-DE

Après en avoir délibéré

Oui l'exposé du rapporteur

LE CONSEIL MUNICIPAL

A l'unanimité

DONNE un avis favorable.

Délibéré en séance les jour, mois et an que dessus.

VILLE DE TARTAS
LANDES - 40400

Le Maire,

Jean-François BROQUÈRES

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

MODELE
CHARTE INFORMATIQUE

Ce modèle ne sert que de « support » à la construction d'une charte informatique interne à la collectivité.

Elle doit être adaptée en fonction des besoins de la collectivité

L'ALPI se dégage de toute responsabilité en cas de reproduction intégrale ou partielle du document.

En application de l'article 33 de la loi n°84-53 du 26 janvier 1984 portant disposition statutaires relatives à la fonction publique territoriale, le Comité Technique a été consulté sur cette Charte en date du .....

Elle a été approuvée par délibération du xxxxxxxxxxxxxx en date du :..... et entre en vigueur à la même date.

1. OBJET DE LA CHARTE INFORMATIQUE

La présente charte a pour objet de :

- déterminer les conditions d'utilisation des moyens ou/et des ressources informatiques mis à disposition par xxxxxxxxxx
- définir les droits et obligations de toute personne utilisatrice de ces outils, dans le respect des droits et libertés de chacun,
- garantir la sécurité, l'intégrité et la confidentialité des données.

Elle est, avant tout, un code de bonnes conduites pour les utilisateurs et a pour objectif :

- d'assurer une information,
- de sensibiliser,
- et d'agir sur des comportements de nature à porter atteinte à l'intérêt collectif de xxxxxxxxxxxx

2. CHAMP D'APPLICATION DE LA CHARTE INFORMATIQUE

2.1 Les utilisateurs concernés

La présente charte s'applique à toute personne autorisée à accéder à tout ou partie des moyens informatiques et de communication de xxxxxxxxxx : agents (sur site ou en télétravail), stagiaires, élus, prestataires extérieurs, public, ...

Elle est :

- remise à tous les utilisateurs contre un récépissé,
- opposable aux tiers utilisant un équipement informatique mis à disposition par xxxxxxxxxx, à titre occasionnel ou permanent,
- communicable sur simple demande.

Les stagiaires en formation remplissent uniquement une attestation sur l'honneur.

2.2 Système d'information et de communication (SIC)

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

xxxxxxxxxxx définit les conditions de mise en place du système d'information et de communication au sein des services.

Celui-ci est notamment constitué des moyens suivants (liste non exhaustive) :

- ordinateurs (fixes ou portables),
- périphériques y compris clés USB, assistants personnels, réseaux informatiques (serveurs, routeurs et connectiques),
- photocopieurs et télécopieurs,
- téléphones, smartphones, tablettes et clés 4G,
- logiciels, fichiers, données et bases de données,
- système de messagerie,
- connexion internet, intranet, extranet, abonnements à des services interactifs,...

3. LES OUTILS DE TRAVAIL MIS À DISPOSITION DES UTILISATEURS

xxxxxxxxxxxx veille à remplacer ou à faire réparer les outils mis à la disposition des utilisateurs.

3.1 Poste informatique

Du matériel informatique est mis à la disposition de chaque utilisateur. Celui-ci est fragile, il convient que chacun en prenne soin.

Il comprend (liste non exhaustive) :

- Unité centrale, écran, souris, clavier, ordinateur portable, ...
- Système d'Exploitation : Windows, Mac OS, ...
- Logiciel(s) : pack bureautique, logiciels de communication, de gestion, applications spécifiques.

3.2 Poste de travail nomade

Lorsque ces matériels sont utilisés à l'extérieur, notamment dans le cadre du télétravail ou en intervention, les utilisateurs en assurent la garde et la responsabilité.

Ils doivent assister xxxxxxxxx, dans toutes les démarches (déclaration d'assurance, dépôt de plainte,...) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

Les utilisateurs ont dans cette hypothèse un niveau de surveillance et de confidentialité renforcé et doivent veiller à ce que des tiers non autorisés ne puissent accéder à ses moyens ni les utiliser.

L'équipement nomade fait l'objet d'une sécurisation particulière par chiffrement. Toute donnée confidentielle, ainsi que les données collectées chez un adhérent, doivent être enregistrées sur un média crypté. À la fin du traitement, les données doivent être supprimées de ce même média.

Lorsqu'un accès à distance est accordé aux utilisateurs, il s'effectue par le biais d'un accès xxxxxxxx leur accordant les mêmes permissions que sur le réseau local de xxxxxxxxxx. Les accès distants aux serveurs, par ssh et le bureau à distance par exemple, se feront uniquement par le biais de cette connexion.

Le contournement de ces moyens techniques d'authentification agréés par tout autre procédé est interdit.

En termes de sécurité et de confidentialité, les utilisateurs sont soumis aux mêmes obligations que les utilisateurs restant sur site. Ils devront suivre toutes les prescriptions complémentaires qui leur seront signifiées.

À l'extérieur de l'enceinte de xxxxxxxxx, lors de toute connexion à des points d'accès Wi-Fi qui ne sont pas de confiance (par exemple à l'hôtel, la gare ou l'aéroport...), préalablement à tout échange de données, les utilisateurs devront se connecter systématiquement par le biais de xxxxxxxxxxx.

3.3 Copieur numérique centralisé

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

Du fait de la richesse de ses fonctionnalités, le copieur numérique centralisé constitue une véritable station de travail informatique dont la sécurité doit être assurée comme celle des postes de travail informatiques.

Dès lors que des informations à protéger transitent par ce type d'appareil, l'ensemble des recommandations et réglementations relatives aux systèmes d'informations s'appliquent.

Les utilisateurs doivent s'abstenir de reproduire, copier, diffuser des pages web, images, photographies, textes ou toutes autres créations protégées par le droit d'auteur.

Une sensibilisation est faite aux utilisateurs afin :

- d'éviter l'impression systématique de mails (et notamment en couleur) ou de documents en version provisoire,
- d'utiliser la fonction « aperçu » avant d'imprimer.

3.4 Téléphonie fixe

L'utilisation du téléphone fixe est réservée à des fins professionnelles.

En cas d'absence, les utilisateurs doivent effectuer un renvoi sur le poste d'un autre utilisateur habilité à recevoir et traiter ses appels ou bien sur le service d'accueil de xxxxxxxxxxxx

L'usage du téléphone fixe pour des communications personnelles est toléré aux conditions qu'il soit ponctuel, qu'il concerne des appels locaux et n'entrave pas l'activité professionnelle des utilisateurs.

3.5 Téléphonie mobile

Un téléphone mobile peut être mis à la disposition des utilisateurs pour un usage strictement professionnel.

À ce titre, l'utilisateur est tenu :

- d'en prendre soin et de se conformer aux prescriptions d'usage, décrites dans la notice d'utilisation fournie avec le téléphone,
- d'informer immédiatement xxxxxxxxx en cas de dysfonctionnement, de blocage ou de vol de l'équipement.

Il est rappelé que selon le code de la route, l'usage d'un téléphone par le conducteur d'un véhicule en circulation est interdit.

Si le téléphone mobile autorise une connexion à l'internet, les utilisateurs devront respecter les obligations et interdictions visées au présent point 4.1 « Internet » ci-dessous.

Si les utilisateurs souhaitent utiliser un téléphone mobile personnel à des fins professionnelles (communications téléphoniques, accès à la messagerie ou à tout site internet relevant de l'activité professionnelle), ils s'engagent à informer au plus tôt xxxxxxx de toute perte ou vol, ou toute autre situation susceptible de laisser un tiers non autorisé accéder aux ressources de xxxxxxxxxxxxx

3.6 Tablette tactile et clé 4 G

Ces équipements peuvent être mis à disposition des utilisateurs pour un usage strictement professionnel.

Toutes les obligations et interdictions applicables aux postes de travail, énoncées ci-dessus s'appliquent à l'utilisation de la tablette tactile ou de la clé 4 G.

La clé 4 G doit être exclusivement branchée sur l'ordinateur professionnel de l'utilisateur.

À l'extérieur de xxxxxxxxxxxxx, les utilisateurs ne peuvent se connecter que sur des accès wifi de l'opérateur choisi pour la téléphonie mobile de xxxxxxxxx dont ils dépendent. En cas d'impossibilité, les utilisateurs veilleront à prendre toutes les précautions lorsqu'ils se connecteront à un réseau wifi ouvert et éviter toute intrusion malveillante et/ou non autorisée.

3.7 Signature électronique et certificat

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

Certains utilisateurs, dans le cadre de leurs fonctions, sont amenés à utiliser des certificats de signature électronique, soit pour :

- signer des documents,
- s'authentifier et accéder à des services sécurisés.

Le certificat, nominatif et non cessible, est constitué de 3 éléments indissociables :

- les informations concernant l'identité du titulaire, son organisation, sa fonction, la période de validité du certificat et l'identité de l'autorité de certification qui l'a généré,
- la clé privée,
- la clé publique.

3.8 Badges électroniques et pointeuse

Les utilisateurs disposent d'un badge électronique nominatif et non cessible permettant d'accéder aux locaux de xxxxxxxxx. Celui-ci est connecté au logiciel de contrôle d'accès du bâtiment qui enregistre les horaires d'entrées et de sorties. xxxxxxxxxxxx pourrait avoir accès à ces données en cas de contrôle.

De la même manière, une pointeuse pour le suivi des horaires de travail des agents est mise en place.

Ces dispositifs ont été portés à la connaissance des utilisateurs avant leur mise en œuvre.

4. LES MOYENS ASSURANT LA SECURITE INFORMATIQUE

4.1 Internet

Les utilisateurs qui disposent d'un accès à l'Internet pour l'exercice de leur activité professionnelle doivent respecter les prescriptions suivantes :

- interdiction d'accéder à des sites illicites : sites à caractère pédophile, raciste, pornographique, ...
- interdiction d'accéder à tout site qui pourrait nuire à l'intérêt de la collectivité dans d'autres domaines,
- interdiction de télécharger des logiciels, des vidéos, des photos n'ayant aucun lien avec les fonctions et activités de xxxxxxxxxx

À des fins de sécurité et de vérification du bon accès et usage des ressources du système d'information, xxxxxxxxxx dispose d'un service de filtrage de contenu Internet (cf article 6.1 de la présente charte).

xxxxxxxxxx accorde une tolérance à l'accès à des sites Internet à des fins personnelles. Elle est permise dès lors qu'elle reste raisonnable c'est-à-dire limitée dans sa fréquence, sa durée et qu'elle ne nuit pas au bon fonctionnement des services.

4.2 Suite antivirale

Les postes de travail sont équipés d'une suite antivirale (antivirus, antispyware, contrôle du web...) choisie par xxxxxxxxxxx

Celle-ci ne constitue pas une protection intégrale contre tous les risques. La vigilance des utilisateurs sur des comportements anormaux reste indispensable.

Comme toute application, un antivirus doit être mis à jour quotidiennement et de façon automatique.

À cet effet, les utilisateurs doivent se conformer aux instructions suivantes :

- il est interdit d'installer un autre antivirus pour quelque raison que ce soit,
- ils doivent veiller à ce que leur poste de travail soit connecté à internet et accepter la mise à jour de l'antivirus : Il ne faut ni l'annuler ni la reporter au moment où elle se présente (risque d'oubli ultérieur).

Les supports amovibles fournis par xxxxxxxxx (cd, clés USB cryptées ou pas, disques durs nomades) sont soumis à un contrôle antivirus préalable à toute utilisation.

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

Une analyse en temps réel est programmée pour contrôler les différents médias amovibles. Toutefois, les utilisateurs doivent scanner régulièrement les différents médias mis en leurs possessions.

L'usage de tout support extérieur est strictement interdit (clé USB personnelle pour un usage professionnel, et inversement).

En cas de changement d'ordinateur, une demande d'installation de l'antivirus officiel de xxxxxxxxx devra être faite à l'adresse mail suivante : xxxxxxx

4.3 Pare-feu

Les postes raccordés à un réseau sont équipés d'un pare-feu individuel (ou firewall) filtrant les accès.

La tâche principale est de contrôler, filtrer, accepter ou bloquer les communications entrantes et sortantes. Il est donc formellement interdit aux utilisateurs de modifier, désactiver ou supprimer ces paramètres de protection.

4.4 Compte « utilisateur » et mot de passe

L'accès aux postes de travail et aux applications s'effectue par un compte nominatif et est protégé par un mot de passe.

Chaque utilisateur est responsable de ses identifiants et mots de passe et de l'usage qui en est fait.

Le mot de passe doit être individuel et rester secret. À cet effet, il ne devra être noté sur aucun support et est, de par sa nature, incessible et intransmissible.

Pour garantir au mieux la confidentialité des fichiers et la sécurité du réseau, xxxxxxxxxx a mis en place :

- une politique de mot de passe rigoureuse. Afin de se conformer aux bonnes pratiques recommandées par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), les mots de passe comportent au minimum 8 caractères alphanumériques (majuscules + minuscules + caractères spéciaux + chiffres) et ne peuvent pas contenir le nom ou une partie du compte utilisateur. Les utilisateurs modifieront les mots de passe tous les 90 jours.

- un nombre maximum de tentatives d'accès à un compte. Lorsque la limite est atteinte, la possibilité d'authentification à ce compte est bloquée temporairement ou jusqu'à l'intervention de l'administrateur du système.

- un paramétrage des postes de travail lors d'une absence prolongée afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité (10 minutes maximum). Toutefois, les utilisateurs doivent verrouiller leur poste de travail lors de tout éloignement de celui-ci afin de préserver la confidentialité des informations traitées.

À la fin de la journée de travail, les utilisateurs doivent impérativement quitter les applications et suivre la procédure d'arrêt complet du système logiciel.

4.5 Messagerie électronique

Les utilisateurs disposent d'une boîte aux lettres nominative permettant de recevoir et d'émettre des messages électroniques uniquement professionnels. Ceux-ci comportent obligatoirement :

- le nom et le prénom de l'expéditeur,
- le service ou le pôle d'appartenance,
- et les coordonnées de xxxxxxxxxxxx

Les utilisateurs doivent :

- veiller à supprimer rapidement les courriels volumineux sans valeur professionnelle et juridique pertinente et à archiver régulièrement la base de messagerie ; le volume des boites et des courriels échangés étant limité,
- vérifier la liste des destinataires,
- prévenir immédiatement leur hiérarchie et l'Administrateur système dans le cas où les utilisateurs recevraient des messages non sollicités, récurrents ou manifestement illicites.

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

xxxxxxxxx se réserve le droit d'effectuer des contrôles dans des cas graves de mauvaise utilisation (la liste suivante n'étant pas exhaustive):

- envoyer ou recevoir délibérément des informations et données dont le contenu et la forme peuvent nuire à xxxxxxxxx
- envoyer des informations confidentielles sur l'organisation, le personnel et les élus de xxxxxxxxxx
- envoyer des messages pouvant engager la responsabilité contractuelle de xxxxxxxxxxxx

Les mêmes dispositions s'appliquent également pour l'utilisation de boîtes aux lettres professionnelles génériques.

En cas d'absence prévisible

Les utilisateurs doivent mettre en place un message automatique d'absence indiquant la date de retour prévue et éventuellement la personne ou le service à joindre en cas d'urgence.

4.6 Archivage électronique

Dans le cadre du développement de l'administration électronique et dans l'objectif de conserver de manière pérenne et intègre les données dématérialisées, xxxxxxxxxx s'est dotée d'une plateforme d'archivage électronique.

La mise en place de cet outil nécessite d'établir une politique d'archivage définissant les objectifs à atteindre et les moyens mis en œuvre.

4.7 Administrateur informatique

Pour veiller à l'intégrité du système informatique, l'Autorité Territoriale a désigné un administrateur informatique.

Il est chargé :

- de l'installation et la gestion des outils et ressources informatiques,
- d'assurer le bon fonctionnement et la sécurité du système pour l'ensemble des utilisateurs,
- de prendre toutes mesures nécessaires et conformes à la réglementation afin de préserver la confidentialité des informations professionnelles ou privées des utilisateurs qu'il est amené à connaître dans le cadre de sa fonction.
- de procéder à toutes les investigations nécessaires. À ce titre, il peut :

    - o générer et consulter tout journal d'évènements et enregistrer des traces si besoin est,

    - o établir des statistiques utiles pour faciliter l'optimisation du système, la sécurité et la détection des abus,
    - o réaliser, selon les services proposés, des sauvegardes de serveurs de production, y compris ceux hébergeant les données des utilisateurs et le courrier électronique,

    - o intercepter tout flux informatique (internet, courriel, transfert de fichier, téléphonie, vidéo...) présentant des risques pour la sécurité (virus, ver, spyware, trojan, wabbit...),

    - o procéder à toute recherche préventive de faille sur les machines branchées sur le réseau interne, et déconnecter, physiquement ou logiquement, lesdites machines en cas de suspicion,

    - o être autorisé à analyser un certain nombre d'éléments relatif au flux de trafic ainsi qu'aux volumes stockés, pour des raisons de prévention et de résolution de problèmes techniques,

    - o être amené à intervenir sur l'environnement technique des postes de travail, dans le cadre des mises à jour et évolution du système d'information.

Il est soumis, dans le cadre de ses fonctions afin de garantir la sécurité du réseau, au devoir de confidentialité vis-à-vis des informations qu'il peut recueillir de manière intentionnelle ou accidentelle.

Par ailleurs, il doit informer les utilisateurs de toutes interventions qu'il serait amené à faire, susceptibles de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques.

Cas exceptionnels

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.

La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

Pour assurer la continuité du service public, l'Administrateur informatique, sur demande de xxxxxxxx peut accéder :

- à la messagerie d'un utilisateur absent en respectant la législation en vigueur et sous certaines conditions : il est notamment interdit à quiconque de prendre connaissance d'un message professionnel ayant pour objet « Personnel » ou « Confidentiel », sans l'autorisation expresse de l'utilisateur (qui en soit l'auteur ou le destinataire).

- aux fichiers pendant l'absence des utilisateurs ; toute mesure devant être prise pour empêcher l'accès aux données identifiées comme personnelles sur les outils de travail.

Par ailleurs, pour des raisons exceptionnelles de sauvegarde de la sécurité, tous les messages professionnels pourront être ouverts par l'Administrateur informatique sur demande écrite de l'Autorité Territoriale.

5. LES DROITS ET DEVOIRS DES UTILISATEURS

5.1 Principes généraux

Les utilisateurs doivent :

- appliquer les recommandations de sécurité inscrites dans la présente Charte,
- respecter les règles de bon usage afin d'éviter des opérations qui pourraient avoir pour conséquence de nuire à xxxxxxxxxxx

À ce titre, ils :

- disposent d'un droit d'accès strictement personnel et incessible,
- contribuent à la sécurité informatique de xxxxxxxxxxx, en signalant tout dysfonctionnement ou toute anomalie des ressources qu'ils utilisent,
- utilisent les logiciels dans le respect des règles relatives à la propriété intellectuelle et des droits d'auteur. Ils ne doivent pas reproduire et/ou ne pas diffuser des données soumises à un droit de copie qu'ils ne détiennent pas,
- ne doivent pas introduire de « ressources extérieures » matérielles ou logicielles qui pourraient porter atteinte à la sécurité du système d'information et de communication,
- effectuent des sauvegardes à échéances régulières pour les fichiers autres que ceux déjà sauvegardés par xxxxxx
- organisent et mettent en œuvre les moyens nécessaires à la conservation des messages électroniques.

L'utilisation des moyens doit se limiter à un usage professionnel dans le cadre des missions de service public de xxxxxxxxxxxxx. Elle doit être réalisée de manière loyale et responsable par tous les utilisateurs.

L'usage à titre personnel doit rester exceptionnel et particulièrement modéré dans sa fréquence et sa durée et ne pas nuire au bon fonctionnement du service.

5.2 Le respect de la confidentialité des données

- Répartition des droits d'accès aux fichiers

Les utilisateurs sont amenés à gérer, du fait de leurs compétences et dans le cadre de leurs missions, des fichiers dont il est nécessaire de garantir la confidentialité : fichiers d'état civil, fichiers d'usagers des services, dossiers individuels et bulletins de paie des utilisateurs...

Ils :

- doivent respecter l'intégrité et la confidentialité des données, tant pour la collecte, le traitement et la communication interne et externe des données,
- ne doivent pas copier ni sauvegarder les fichiers professionnels sur support amovible autres que ceux fournis par xxxxxxxxxxxxx
- ne peuvent collecter des données qui, en raison de leur contenu, contreviendraient aux lois et règlements en vigueur.

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

Une organisation est mise en place pour interdire l'accès aux fichiers confidentiels à toute personne autre que le ou les gestionnaires desdits fichiers.

- La protection des données personnelles informatiques

Un nouveau règlement de l'Union européenne, appelé le Règlement Général sur la Protection des Données ou « RGPD », accorde aux personnes privées (les utilisateurs) certains droits relatifs à leurs données personnelles qui sont :

- droit d'accès : le droit d'être informé et de demander l'accès aux données personnelles que xxxxxxxxx traite,

- droit de rectification : le droit de demander de modifier ou de mettre à jour les données personnelles lorsqu'elles sont inexactes ou incomplètes,

- droit d'effacement : le droit de demander de supprimer définitivement les données personnelles,
- droit de restriction : le droit de demander d'arrêter temporairement ou définitivement le traitement de tout ou partie des données personnelles,

- droit d'opposition :

  - le droit de refuser à tout moment le traitement des données personnelles pour des raisons personnelles,

  - le droit de refuser le traitement de vos données personnelles à des fins de marketing direct,

- droit à la portabilité des données : le droit de demander une copie de vos données personnelles au format électronique et le droit de transmettre ces données personnelles pour une utilisation par un service tiers,

xxxxxxxxxxx a pris en compte ces nouvelles directives. Les utilisateurs peuvent exercer ces droits en utilisant l'adresse : xxxxxxxxxx

5.3 En cas de départ d'un utilisateur

Tout utilisateur, lors de la cessation de son activité au sein de xxxxxxxxxx, perd son habilitation à utiliser le SIC.

Il doit :

- restituer tous les matériels mis à sa disposition,
- effacer de son poste de travail tous ses fichiers et données privées.

Il ne peut effectuer une copie de son travail professionnel qu'après autorisation écrite de son supérieur hiérarchique dûment habilité.

Le répertoire personnel des utilisateurs situé sur le serveur sera obligatoirement supprimé par l'administrateur informatique, en tout état de cause dans un délai maximum de trois (3) mois après son départ.

6. CONTRÔLE DE L'UTILISATION DES MOYENS D'INFORMATION ET DE COMMUNICATION

6.1 Solution de filtrage des contenus

Face aux risques et menaces de plus en plus sophistiquées, xxxxxxx a mis en place à compter du xxxx, le filtrage des contenus filtrant les sites web visités et permettant de logguer (journaliser) les actions utilisateurs.

À ce titre, le filtrage concernera l'ensemble des utilisateurs et permet de :

- renforcer la sécurité des systèmes d'information (Analyse des menaces, antispyware...),

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

- interdire l'accès à des sites illicites : sites à caractère pédophile, raciste, ...
- interdire l'accès à tout site qui pourrait nuire à l'intérêt de la collectivité dans d'autres domaines,
- assurer une meilleure qualité de service en contrôlant l'utilisation de la bande passante : interdiction de télécharger des logiciels, des vidéos, des photos n'ayant aucun lien avec les fonctions et activités de xxxxxxxxxxxxx
- empêcher la divulgation d'informations : En effet, dans le cadre de leurs fonctions, les utilisateurs sont amenés à gérer des fichiers dont il est nécessaire de garantir la confidentialité : fichier d'état civil, fichiers d'aide sociale, bulletins de paie, ...
- protéger : le filtrage n'a pas pour effet de contrôler l'activité sauf dans le cas de présomptions d'infractions aux règles de sécurité énoncées dans la présente charte ou d'abus,
- protéger xxxxxxxxxx : en effet, dans l'hypothèse où il n'est pas mis en place de solution de filtrage, la responsabilité de xxxxxxxxx peut être engagée pour des infractions commises par les utilisateurs dans l'exercice de leurs fonctions (risque civil et pénal),
- respecter les obligations juridiques : différents textes de lois ou références juridiques imposent le recours au filtrage comme la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique qui impose à certains acteurs de mettre en œuvre des moyens de contrôle ou de restriction des accès à internet.

- Fonctionnement du filtrage

La solution de filtrage retenue est la solution xxxxxxxxxxx et l'outil est installé sur tous les postes de travail (sur sites et nomades).

La période de filtrage sur les postes de travail s'étend sur toute la journée (temps de pause comprises) et depuis n'importe quel accès internet (Maison des Communes, domicile, télétravail, site extérieur,...).

Il est formellement interdit de modifier, désactiver ou de supprimer ces paramètres de filtrage et de blocage.

- Blocages de sites

Plusieurs politiques de filtrages ont été établies sur la base d'un classement par catégories de sites autorisés, bloqués ou soumis à un quota d'utilisation.

En cas de blocage, Il apparaît la bannière ci-dessous (**Exemple 1 : page de blocage**). Sur certaines bannières, un bouton « **Poursuivre** » permettra, comme son nom l'indique, de poursuivre la navigation.

- Demandes de déblocage de site

Les révisions éventuelles des politiques de filtrage seront adoptées après accord de l'Autorité territoriale.

Les faux positifs (= sites bloqués qui doivent être débloqués pour l'exercice des missions) devront être signalés à l'adresse mail générique suivante : xxxxxxxxxxxxxxx

- Archivage des traces/Gestion des logs /Statistiques

La solution de filtrage permet l'établissement de statistiques par groupes d'utilisateurs, et la génération de journaux selon différents critères :

- temps de navigation,
- bande passante consommée,
- nombre d'accès,
- catégories d'URL consultées.

En cas d'abus ou de doutes sur l'utilisation d'internet, les fichiers sont conservés afin d'engager une procédure interne de contrôle.

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

- Procédure interne de contrôle

En cas de doute ou de présomptions d'infractions ou de connexions abusives pendant les heures de travail, l'autorité territoriale peut interdire ou suspendre l'accès aux ressources prévues et être amené à effectuer des contrôles conformément aux règles édictées dans la présente Charte.

Tout contrôle et toute sanction font l'objet d'une information préalable de la personne suspectée.

6.2 En cas de faute

xxxxxxxxx a la responsabilité des fautes commises par ses utilisateurs dans le cadre de leurs missions.

À ce titre, elle souscrit un contrat d'assurance de protection juridique. Celui-ci est également indispensable quand l'utilisateur fait l'objet de poursuites pénales à l'occasion de faits qui n'ont pas le caractère de faute(s) détachable(s) de sa fonction.

Elle pourra prendre les mesures et sanctions appropriées.

Xxxxxxxxx est exonérée de toute responsabilité lorsque l'utilisateur agit en dehors de ses fonctions, sans autorisation et à des fins étrangères à ses attributions.

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

3. BASES LEGALES

Les principales dispositions légales en vigueur prévues par la législation française et européenne sont notamment les suivantes :

- Le règlement (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractères personnel et à la libre circulation de ces données,
- La loi n°78-17 du 06/01/78 dite « Informatique et liberté » modifiée par la loi n°2018-493,
- Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques,
- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,
- La législation relative à la propriété intellectuelle,
- La législation relative à la fraude informatique,
- La législation en matière de transmission d'informations à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine et à la diffusion de contenus illicites à caractère injurieux, diffamatoire, raciste, xénophobe, révisionniste et sexiste (articles 227-23 et 227-24 du Code Pénal et loi du 29 juillet 1881),
- Décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques,
-
- Loi n°84-53 du 26 janvier 1984 (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 utilisateurs non titulaires,
- Décret n°91-298 du 20 mars 1991 (art. 15) relatif aux utilisateurs à temps non complet.

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.

Envoyé en préfecture le 05/07/2019
Reçu en préfecture le 05/07/2019
ID : 040-214003139-20190611-2019_C13-DE

RECEPISSE DE LA CHARTE INFORMATIQUE

Je soussigné(e)

Nom : .....

Prénom : .....

Pôle : ..... Fonction : .....

En tant qu'utilisateur du Système d'Information et de Communication de xxxxxxxxxx déclare :

- avoir pris connaissance de la présente charte
- m'engage à la respecter pendant toute la durée de mes fonctions, et sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

Fait à ..... Le .....

Signature

La présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de Pau dans un délai de deux mois à compter de sa publication et de sa réception par le représentant de l'Etat dans le département.
La présente délibération sera transmise à Monsieur le Préfet des Landes.