Accusé de réception en préfecture
001-210104279-20240918-20241809RHIN103-DE
Date de télétransmission : 20/09/2024
Date de réception préfecture : 20/09/2024

TRÉVOUX
DOMBES SAÔNE VALLÉE

CHARTE INFORMATIQUE COMMUNALE

LE CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à tout utilisateur du Système d'Information et de communication de la commune de Trévoux pour l'exercice de ses activités professionnelles que l'accès soit à partir du réseau interne ou à distance.

La charte est diffusée à l'ensemble des utilisateurs par courriel et par une note de service.
Elle est systématiquement remise à tout nouvel arrivant dans sa boite mail et remise sous forme de livrable lors de l'accueil institutionnel.

LES DROITS D'ACCÈS

Ils sont liés au poste.

L'attribution faite à un agent d'outils informatiques et de télécommunication dépend de ses missions.

Décidé par la Direction à laquelle il appartient, ce droit est attribué en fonction des besoins exigés par le poste occupé.

Ce droit d'accès est personnel et incessible, il est strictement limité à des activités professionnelles.

Lorsque l'agent change de poste, les droits d'accès sont mis à jour. L'agent n'utilise plus alors les applications qui ne sont plus du périmètre de ses nouvelles fonctions.

LES DROITS ET OBLIGATIONS

Aucune utilisation des ressources informatiques et de télécommunication ne doit être contraire aux obligations professionnelles des agents, notamment les obligations de réserve, de discrétion professionnelle, de neutralité, de laïcité et de dignité.

Ainsi la consultation de sites, et le stockage ou la diffusion d'informations ou documents pouvant notamment être qualifiés d'injurieux, diffamatoire, discriminatoire, à caractère sexuel, incitant à la violence ou à la haine sont strictement interdits.

L'utilisation de ces ressources ne doit en aucun cas être de nature à porter atteinte à la réputation de la Commune de Trévoux.

Accusé de réception en préfecture
001-210104279-20240918-20241809RHIN103-DE
Date de télétransmission : 20/09/2024
Date de réception préfecture : 20/09/2024

Les fichiers professionnels doivent impérativement être enregistrés sur les espaces sauvegardés. Aucun document professionnel ne doit être stocké sur le disque dur de l'ordinateur et/ou tout support externe.

L'usage des moyens informatiques et de télécommunication de la commune de Trévoux à des fins personnelles est toléré à condition de rester modéré et raisonnable, et de ne perturber ni la sécurité et la fluidité du système informatique de la commune, ni les missions de l'agent et de son service. Leur usage dans un but commercial est interdit.

Les courriels personnels ou privés (ci-après nommés courriels « privés ») générés par la messagerie professionnelle de l'agent sont couverts par le secret des correspondances privées (article 226.15 du nouveau Code pénal qui protège le secret des « correspondances émises, transmises ou reçues par la voie des télécommunications »).

Les courriels privés sont ceux qui sont identifiés comme tels de manière claire, par exemple par la mention « personnel » ou « privé », et/ou dont le contenu concerne de manière évidente la vie privée de l'agent. A défaut, les courriels sont présumés professionnels.

Les agents ne peuvent, à moins d'y avoir été autorisés par la personne concernée, prendre connaissance, enregistrer ou transmettre, par quelque moyen que ce soit, des communications, correspondances, fichiers et plus généralement toutes informations détenues par d'autres agents.

Le service informatique a accès à l'ensemble des données et peut être amenés à accéder à des informations privées. Ils ont l'obligation professionnelle de préserver la confidentialité de ces informations.

Sauf risque ou évènement et particulier, la commune de Trévoux ne pourra ouvrir les fichiers et courriels privés qu'en présence de l'agent ou celui-ci dûment appelé.

En cas d'absence prolongée et imprévue supérieure à une semaine de l'agent, le service informatique, sur demande expresse de la Direction Générale, mettra en œuvre les moyens techniques de gestion de la messagerie afin d'assurer la continuité de service.

Par ailleurs, pour toute absence inférieure, la commune de Trévoux peut accéder à la boîte aux lettres électronique et aux dossiers et fichiers présents sur les outils informatiques utilisés par l'agent en cas d'absence de ce dernier, afin d'assurer la continuité du service. Cet accès se fait, après information de l'agent, par un supérieur hiérarchique ou de son suppléant par nécessité d'intervention. Seuls les messages et fichiers de nature professionnelle en lien direct avec l'activité du service devront être consultés dans ce cadre.

GESTION EFFICIENTE DE LA MESSAGERIE

Respecter les circuits et l'organisation et/ou la voie hiérarchique le cas échéant.

Renseigner explicitement l'objet pour le destinataire dans le respect notamment du devoir de neutralité et de l'obligation de discrétion professionnelle.

Eviter les messages trop volumineux et le stockage excessif.
Pour envoyer par Internet un fichier volumineux ou de nombreuses pièces jointes, l'utilisation d'un outil d'archivage est à privilégier pour ne faire qu'une pièce jointe compactée (fichiers ZIP).

Accusé de réception en préfecture
001-210104279-20240918-20241809RHIN103-DE
Date de télétransmission : 20/09/2024
Date de réception préfecture : 20/09/2024

Être un destinataire actif et responsable : Lire régulièrement les messages reçus ; En cas d'absence prolongée (congés, formation, etc.), information des interlocuteurs grâce au gestionnaire d'absence du bureau.

Respecter la capacité limitée de chaque boîte aux lettres.

Détruire immédiatement les messages qui ne sont pas importants.

Archiver les pièces jointes avec suppression de la messagerie.

Gérer mes Spams et les courriers indésirables : Dans ce cas, aucune réponse ne doit être apportée et **l'attache immédiate est prise avec le service informatique** pour vérifier le bon fonctionnement et lutter contre la propagation des messages non désirés. Plus généralement, s'il existe un doute quelconque sur un message parvenant à un agent, la bonne pratique est de le supprimer sans l'ouvrir ceci afin d'éviter tout problème qui pourrait être lié au contenu de ce message.

DROIT À L'IMAGE DES AGENTS

Les informations relatives au droit à l'image des agents sont disponibles dans le document « Information du salarié et droit à l'image ». Ce document, remis par le service des Ressources Humaines, doit être signé par chaque agent à son arrivée dans la collectivité.

GESTION INTERNET / INTRANET

Pour assurer une bonne disponibilité du service Internet et limiter l'accès à ces sites, un mécanisme de filtrage automatique de sites non professionnels ou illégaux est effectué. Ce filtrage n'est cependant pas absolu s'agissant des sites non professionnels pour permettre la navigation modérée et raisonnable sur le réseau Internet à des fins personnelles.

Certains usages consomment beaucoup de bande passante, c'est pourquoi, (dans **le cadre d'un usage privé)**, il est interdit notamment de :

- Télécharger ou de visionner des films et vidéos.
- Télécharger des œuvres musicales.
- Télécharger des logiciels et des mises à jour de logiciels hormis les logiciels métiers.
- Regarder des programmes télévisés en direct ou en replay.
- Ecouter des radios, de la musique, en direct ou en replay.
- Gérer des espaces **personnels** de stockage hébergés sur des sites internet : Dropbox, Google drive, icloud…etc…
- Gérer des réseaux sociaux ou des blogs **personnels** : Facebook, Twitter, Tumblr…

MOYENS DE SUPERVISION ET DE CONTRÔLE

Le Service Informatique (ou son prestataire) et Télécommunications est responsable de la sécurité du système d'information et du bon fonctionnement des moyens de communication de la Ville de Trévoux. Il doit assurer une disponibilité maximale des différents moyens qu'elle met à la disposition des agents et le respect des budgets alloués.

Accusé de réception en préfecture
001-210104279-20240918-20241809RHIN103-DE
Date de télétransmission : 20/09/2024
Date de réception préfecture : 20/09/2024

Ces préoccupations techniques et budgétaires l'amènent par exemple à veiller à l'encombrement global des boîtes aux lettres, au stockage des données, à la saturation de l'accès à Internet, et aux consommations téléphoniques.

Les informations et données suivantes émanant de l'utilisation des outils informatiques et de télécommunication à la disposition des agents sont enregistrées.

Lorsqu'un agent accède à Internet, le serveur de connexion enregistre :

- **L'identifiant** de l'utilisateur sous la forme de son code d'accès au système d'Information • **L'adresse** du site web visité
- **Le nombre d'accès** à ce site par l'utilisateur
- **Le pourcentage des accès** par rapport au nombre d'accès total pour cet utilisateur
- **Le nombre de sessions** ouvertes par l'utilisateur
- **La durée totale** de l'activité de l'utilisateur
- **Le volume des données** transmises par l'utilisateur.

- **Mode de contrôle :**

Le service informatique ou les prestataires habilités procèdent aux investigations et au contrôle de l'utilisation des outils Informatiques et de télécommunications afin notamment d'assurer la sécurité, la disponibilité du réseau et la maîtrise des dépenses.

En cas d'atteinte aux règles énoncées dans la présente charte, le service informatique aura la charge d'avertir l'utilisateur et informera le directeur concerné.

Cette procédure de contrôle peut également être engagée sur demande du supérieur hiérarchique.

Dans l'hypothèse où le service informatique constaterait un comportement susceptible d'engager la responsabilité pénale d'un agent, le responsable hiérarchique sera informé immédiatement.

- **Conservation et consultation des données :**

Concernant les connexions à Internet, les données enregistrées par le serveur de connexion sont conservées sur support numérique pendant une durée de 12 mois à compter de la date de leur collecte.

Ces informations collectées pourront être transmises aux services de Police ou du Procureur de la République si les agissements en cause sont susceptibles d'être qualifiés d'infraction pénale.

SÉCURITÉ INFORMATIQUE

D'une manière générale, la sécurité informatique vise à garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité du système d'information.

Afin d'aider à atteindre ces objectifs de sécurité chaque utilisateur s'engage à :

Ne pas modifier la configuration de son poste de travail sans l'accord du service informatique ou du prestataire : pas d'installation de logiciels, pas d'ajout de matériels. L'homogénéité des postes de travail est en effet une condition indispensable pour maîtriser l'intégration des composants, leur déploiement, leur administration et donc leur disponibilité.

Accusé de réception en préfecture
001-210104279-20240918-20241809RHIN103-DE
Date de télétransmission : 20/09/2024
Date de réception préfecture : 20/09/2024

Chaque poste de travail correspond à une configuration type, adaptée à votre profil professionnel (applications auxquelles vous avez accès). Si une réinstallation est nécessaire, elle sera faite sur les bases de cette configuration répertoriée.

Ne pas effectuer d'opérations pouvant nuire au bon fonctionnement des systèmes et à leur intégrité (intervention sur des fichiers systèmes, par exemple).
Vous êtes en effet responsable de l'utilisation que vous faites des ressources informatiques.

La clé dans le système d'information est composée d'un identifiant et d'un mot de passe ; ces informations sont strictement personnelles et ne doivent en aucun cas être communiquées à quiconque (Collègue, supérieur hiérarchique). En effet, l'identifiant de chaque utilisateur lui donne droit d'accéder à la partie du système d'information correspondant aux fonctions et responsabilités exercées. Ce couple identifiant/mot de passe ne doit jamais être inscrit en clair sur un support accessible à autrui (Papier, fichier informatique sur un espace bureautique, post-it…).

Pour consolider cette confidentialité, il est obligatoire de changer le mot de passe régulièrement lorsque le système d'information vous invite à le faire. Une fois ce changement effectué, le service informatique doit en être informé.

D'autres identifiants pourront être personnellement fournis à un utilisateur pour accéder par exemple à des applications ; chaque utilisateur s'engage dans ce cadre à ne se connecter qu'avec le ou les identifiants qui lui ont été personnellement attribués pour un système ou une application donnée.

Dans tous les cas, le service informatique ou son prestataire agréé dispose de la liste nominative des identifiants et mots de passe de tous les utilisateurs.

<u>Tout utilisateur s'engage à respecter les règles de sécurité suivantes :</u>

- Signaler au service informatique toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.
- Ne jamais confier son identifiant/mot de passe à quiconque.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramétrages du poste de travail.
- Ne pas installer de logiciels sans autorisation.
- Ne pas copier, modifier, détruire les logiciels propriétés de la commune de Trévoux.
- **Verrouiller** son ordinateur dès qu'il quitte son poste de travail.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Ne pas effectuer de copie de données sur un support externe sans l'accord de son supérieur hiérarchique.
- Ne pas stocker, de données professionnelles sur un hébergement autre que le système d'information de Trévoux.
- Ne pas utiliser d'outils informatiques en ligne sans avoir pris connaissance des conditions d'utilisation et sans l'aval de votre service informatique.
- Ne pas ouvrir de mails ou de fichiers de provenance inconnue, d'apparence inhabituelle ou frauduleuse.
- Ne pas cliquer sur des liens de provenance inconnue présents dans les mails.
- Ne pas ouvrir de pièces jointes à des mails de provenance inconnue ou suspecte.