Envoyé en préfecture le 06/11/2024
Reçu en préfecture le 06/11/2024
Publié le
ID : 974-219740149-20241029-DCM134_2024-DE

Charte informatique de la Commune de Saint-Louis

Ce document appartient à la Commune de Saint-Louis et est confidentiel

Il est rédigé à l'attention des *Utilisateurs*, c'est-à-dire des dirigeants et agents de la Commune.

Toute modification et mise à jour sera communiquée à l'ensemble des *Utilisateurs*.

Sommaire

Envoyé en préfecture le 06/11/2024
Reçu en préfecture le 06/11/2024
Publié le
ID : 974-219740149-20241029-DCM134_2024-DE

1. Objet de la charte

Le système d'information de la Commune de Saint-Louis comprend un ensemble de ressources qui sont mises à la disposition de ses *Utilisateurs* pour l'accomplissement de leurs missions professionnelles.

La Commune définit et met en œuvre les moyens appropriés pour en assurer le bon fonctionnement et la sécurité, en adéquation constante avec l'évolution de la technique, du cadre réglementaire et des risques qu'une négligence ou mauvaise utilisation des ressources peut faire courir à la fois à la Commune de Saint-Louis (ex. pertes financières, atteinte à la réputation, etc.) et à l'*Utilisateur* lui-même.

La présente charte définit les droits et les devoirs des *Utilisateurs* du système d'information de la Commune. Elle a pour objectifs d'encadrer les usages des ressources mises à disposition, de sensibiliser les *Utilisateurs* aux risques de sécurité, de préciser les responsabilités de chacun, et d'informer les *Utilisateurs* sur les contrôles menés par la Commune.

Cette charte expose ainsi les principes et règles de sécurité et de bon usage auxquels se soumet impérativement tout *Utilisateur* accédant aux ressources du système d'information de la Commune de Saint-Louis quel que soit l'équipement confié. Par ailleurs, elle identifie les dispositions de contrôle mises en œuvre dans le respect des droits fondamentaux des *Utilisateurs*.

2. Champ d'application de la charte

Cette charte présente les principes généraux et fondamentaux qui devront être appliqués par les *Utilisateurs* concernés lors de leur utilisation des ressources informatiques de la Commune.

La charte s'applique à l'ensemble des *Utilisateurs* du système d'information de Saint-Louis quel que soit son statut (agent, stagiaire, élu…) ou sa localisation (au sein ou hors des locaux de la Commune).

Les principes et règles définis par la présente charte s'appliquent aux données, ainsi qu'aux ressources mises à disposition des *Utilisateurs* par la Commune de Saint-Louis :

- Les équipements informatiques : ordinateurs fixes ou portables, imprimantes multifonction, terminaux mobiles et appareils assimilables (smartphones, tablettes numériques, etc.) ;
- L'accès aux réseaux informatiques ;
- Les applications ainsi que les services de communications (messagerie électronique, messagerie instantanée, solutions de transferts de fichiers, etc.) ;
- Les supports d'information amovibles (clés USB, disques durs externes, etc.).

Toute manœuvre non autorisée sera considérée comme violation à l'engagement faisant l'objet du présent document.

3. Engagement de respect de la charte et sanctions

Tout *Utilisateur* du système d'information de la Commune de Saint-Louis s'engage à respecter l'ensemble des principes, règles et obligations tels que figurant dans la présente charte. A

défaut, il engage sa responsabilité personnelle. L'*Utilisateur* fautif s'expose à d'éventuelles sanctions de nature disciplinaire, appropriées et proportionnées sans préjuger des actions complémentaires pouvant être engagées à son encontre sur le plan civil et pénal selon les lois locales.

En cas de doute quant à l'application des règles de la présente charte, l'*Utilisateur* contacte le service informatique.

4. Obligations légales

Toutes les structures et tous les *Utilisateurs* doivent se conformer et respecter les lois et les règlements nationaux en vigueur du pays de rattachement auxquelles elles appartiennent.

5. Règles de sécurité et de bon usage des ressources

5.1. Respect des règles de sécurité

Ce chapitre est un condensé de notions qui seront détaillées dans la suite du document.

De manière générale, chaque *Utilisateur* a une responsabilité de sécurité des ressources mises à sa disposition ou utilisées, et une responsabilité collective quelle que soit sa mission au sein de la Commune. Chaque *Utilisateur* doit **adopter un comportement en accord avec les principes de base de sécurité**.

Il doit en particulier :

- Respecter les règles de sécurité applicables aux différentes ressources qui lui sont confiées ou auxquelles il a accès ;
- Veiller à la sécurité des accès qui lui sont donnés (comptes et mots de passes ou tout autre moyen d'authentification, etc.), en se conformant aux politiques en vigueur et en s'assurant de ne les partager avec personne, que ce soit à l'intérieur ou à l'extérieur de la Commune de Saint-Louis ;
- Surveiller et garder en sécurité, en toutes circonstances, les équipements mis à sa disposition ;
- Ne pas connecter un équipement personnel au réseau de Saint-Louis, sauf demande expresse au service informatique de la Commune de Saint-Louis ;
- Verrouiller ou déconnecter ses dispositifs en cas d'absence (même temporaire), et les éteindre en cas d'absence prolongée.

Chaque *Utilisateur* doit rester **vigilant dans son utilisation** des ressources informatiques et outils numériques mis à sa disposition. Son attention est en particulier attirée sur :

- L'utilisation du système de communication, avec d'autres collaborateurs comme avec des tiers, qui doit se faire avec la plus grande prudence et où tout échange ou document suspect doit être immédiatement signalé au service informatique ;
- Les précautions à prendre en cas de déplacement, de passage dans des lieux publics, d'utilisation de réseaux hors ceux de Saint-Louis, afin d'éviter tant la fuite d'informations sensibles que la perte ou le vol de ressources.

Enfin chaque *Utilisateur* doit **avoir une attitude de coopération** avec les équipes responsables de la gestion de la sécurité du système et des ressources de la Commune. Il se doit ainsi de respecter les instructions permanentes ou ponctuelles du service informatique pour garantir la sécurité et le bon fonctionnement des ressources informatiques. Inversement, il ne doit en aucun cas :

- Contourner les moyens de sécurisation ou de filtrage des ressources mis en place par la Commune (ex. plateformes d'accès sécurisé, anti-virus, proxy), ou nuire à leur bon fonctionnement. Il est rappelé que seul le service informatique est autorisé à effectuer des opérations de maintenance sur les équipements informatiques ;
- Introduire ou exploiter des failles de sécurité dans le système, par exemple par la connexion d'un équipement inconnu sur le réseau ;
- Tenter de modifier, désactiver ou contourner les mécanismes de sécurité mis en œuvre (logiciel antivirus, écran de veille automatique, outils d'authentification, outils de chiffrement de données ou de messages, etc.) ;
- Utiliser ou tenter d'utiliser des outils de sécurité non-fournis par la Commune, notamment en termes de sécurité réseau ou de chiffrement de données autre que ceux fournis et/ou autorisés, de sorte que les données professionnelles demeurent accessibles en l'absence de l'*Utilisateur* pour répondre aux besoins de continuité d'activité ou de réquisition judiciaire.

L'*Utilisateur* doit communiquer tout incident de sécurité quel qu'il soit (présence de virus, réception de pièces jointes suspectes, site web dangereux non bloqué, perte ou vol d'équipement, etc.). Il doit signaler sans délai à l'équipe chargée de traiter ces événements par téléphone.

5.2. Tolérance de l'utilisation à des fins privées

L'utilisation des ressources à des fins privées est tolérée de manière occasionnelle pour répondre aux nécessités de la vie courante et familiale (par exemple, en France la notion de « vie privée résiduelle »), sous réserve que cet usage :

- Reste raisonnable ;
- N'affecte pas les conditions d'accès, le bon fonctionnement ou la sécurité des services concernés ;
- Ne mette pas en cause la productivité de l'Utilisateur dans l'accomplissement de ses missions professionnelles ni celle de ses collègues ;
- Ne puisse en aucun cas nuire aux intérêts ni à l'image de la Commune de Saint-Louis ou bien encore porter un quelconque préjudice à un tiers ;
- N'occasionne pas de frais et/ou d'investissements supplémentaires (ex. moyens financiers, techniques ou humains nécessaires au rétablissement des moyens de travail ou facturation liée à des outils de mobilité ne rentrant pas dans le cadre de la mission) ;
- Reste conforme à la présente charte, aux dispositions légales, au contrat de travail et aux règles impératives fixées par la Commune à laquelle l'Utilisateur est rattaché.

L'ensemble des données produites, traitées et stockées sur le système d'information de la Commune de Saint-Louis est présumé à caractère professionnel. Le cas échéant, tout élément à caractère privé présent sur le système d'information, qu'il soit électronique (email, dossier, fichier, etc.) ou physique (impression, courrier, etc.), doit être identifié par l'*Utilisateur* en y attachant la mention « Privé », « Perso », « Personnel », ceci afin que les principes de secret de la correspondance et de respect de la vie privée de l'*Utilisateur* puissent être appliqués. Dans le cas de fichiers à caractère privé, ils devront être contenus dans un dossier spécifique et stocké localement sur le poste de travail et non pas dans des dossiers de partage sur le réseau de la Commune. L'*Utilisateur* est informé que la Commune ne garantit pas la sauvegarde de ces données.

Le respect de la vie privée des *Utilisateurs* est régi selon les lois et les réglementations Françaises.

De façon exceptionnelle, conformément à la loi, et en ayant au préalable sollicité la présence ou l'autorisation de l'*Utilisateur,* le service informatique pourra accéder ou donner accès aux

données non professionnelles (fichiers, messages, etc.) présentes sur les dispositifs et périphériques appartenant à la Commune, et ce dans les cas suivants :

- Demande des autorités judiciaires ;
- Danger imminent menaçant les intérêts de la Commune de Saint-Louis (situation portant préjudice au groupe ou à sa capacité de mener ses activités).

5.3. Accès aux salles serveurs

L'accès aux salles serveurs étant restreint, toute personne qui désire y accéder doit demander l'autorisation au service informatique.

5.4. Postes de travail

La Commune de Saint-Louis met à disposition de ses *Utilisateurs* des postes de travail (ordinateurs fixes, ordinateurs portables ou tablettes hybrides) destinés à l'accomplissement de leur mission professionnelle. Ces postes de travail sont paramétrés et administrés à cet effet par le service informatique de la commune de Saint-Louis.

5.4.1. Règles relatives à la protection physique des postes de travail

L'*Utilisateur* est responsable de la sécurité physique des postes de travail qui lui sont confiés dans le cadre de sa mission. Dans ce cadre, l'*Utilisateur* veille à avoir une utilisation respectueuse de ceux-ci (ex. éviter les chocs, ne pas manipuler de liquides à proximité, placer le matériel dans un lieu sûr et stable) et s'engage à prendre les mesures adaptées pour réduire les risques de casse, perte ou vol notamment lors de ses déplacements.

Principe du bureau propre

A la fin de son travail, sauf exception, l'*Utilisateur* s'engage à ne laisser en vue sur son bureau de travail, aucun actif important ou ayant de la valeur (ordinateurs portables, téléphones portables, mot de passe, documents confidentiels, etc.).

5.4.2. Règles relatives à la sécurisation des postes de travail

5.4.2.1. Un accès individuel

L'accès aux fonctionnalités des applications logicielles nécessite une authentification établie sur la base d'un identifiant, et d'un mot de passe.

Les identifiants sont strictement confidentiels et ne doivent pas être communiqués à une tierce personne.

Il est précisé que l'usage de ses identifiants est fait sous l'entière responsabilité de l'*Utilisateur*. Ainsi, toute connexion, transmission ou utilisation de données effectuée à l'aide de ses identifiants sera présumée avoir été réalisée par l'*Utilisateur* lui-même.

5.4.2.2. Les mots de passe

L'*Utilisateur* ne doit pas utiliser les mêmes mots de passe dans la sphère personnelle et professionnelle et, si possible, choisir un mot de passe différent par système et/ou application. Les mots de passe doivent respecter les consignes de sécurité de la Commune de Saint-Louis concernant leur longueur et leur complexité, et ne pas pouvoir être devinés facilement.

La construction des mots de passe doit respecter les points suivants :

- La longueur minimale d'un mot de passe doit être de **12 caractères ;**
- Le mot de passe **ne doit pas contenir le nom/prénoms de l'*Utilisateur* ;**
- Le mot de passe **doit être différent des cinq derniers mots de passe utilisés.**

Il doit également respecter au moins trois des critères suivants :

- Contenir des caractères **minuscules ;**
- Contenir des caractères **majuscules ;**
- Contenir des **chiffres ;**
- Contenir des **caractères spéciaux.**

5.4.2.3. Confidentialité des mots de passe

Les mots de passe ne doivent, en aucun cas, être notés, gardés au bureau ou stockés sous quelque forme que ce soit, excepté dans les solutions fournies à cette fin par la Commune de Saint-Louis (coffre-fort de mots de passe). En cas de doute sur l'intégrité d'un mot de passe, *l'Utilisateur* doit lancer la procédure de réinitialisation dans les meilleurs délais.

5.4.2.4. Révision des mots de passe

L'*Utilisateur* devra procéder au changement de ses mots de passe s'il lui semble qu'une tierce personne en a pris connaissance.

En sus, pour des raisons de sécurité, il pourra être demandé à l'utilisateur **de réviser ses mots de passe à une fréquence définie par le service informatique.** En cas de suspicion d'un risque de sécurité, le service informatique se réserve le droit de demander le changement immédiat dudit mot de passe.

5.4.2.5. Fermeture de sessions

Les sessions ainsi que ses applications logicielles sont régies par un même et seul mot de passe utilisateur, il est donc impératif de prendre soin de verrouiller sa session de travail ( **+ L** pour Windows**)** durant les pauses et toutes autres circonstances d'absence, aussi courtes soient-elles.

5.4.3. Règles relatives à l'utilisation des ressources personnelles pour l'activité professionnelle

L'utilisation des ressources personnelles n'est autorisée que sous autorisation du service informatique.

Toute autorisation de ce type peut être révoquée à tout moment par le service informatique, en particulier si l'utilisation faite de la ressource personnelle cesse d'être conforme à celle pour laquelle l'autorisation a été accordée.

Il est à noter que la Commune de Saint-Louis n'a ni la responsabilité ni l'obligation d'assurer le support de ressources personnelles ou tierces, et décline toute responsabilité vis-à-vis de l'utilisateur quant à l'utilisation de ces ressources.

Toute ressource personnelle utilisée dans le cadre de l'activité professionnelle pourra en revanche faire l'objet d'obligations (notamment en matière de sécurité) et de contrôles de conformité vis-à-vis de ces obligations.

Il est interdit aux *Utilisateurs* de connecter leur ordinateur personnel au réseau interne de la Commune de Saint-Louis.

5.4.4. Règles relatives à l'interdiction de prêt et revente d'équipement, logiciel ou licence

L'*Utilisateur* ne doit pas, à titre personnel, prêter, vendre ou céder à des tiers, les logiciels, licences, programmes d'installation et outils fournis par la Commune.

L'*Utilisateur* ne doit pas prêter, louer, vendre ou céder à des tiers les équipements fournis par la Commune.

5.4.5. Règles relatives à la sauvegarde des données

L'*Utilisateur* doit veiller à ce que toutes les données professionnelles soient sauvegardées sur une ressource réseau de la Commune, ou à défaut une solution Cloud mise en place par la Commune (Office 365). L'*Utilisateur* doit proscrire le stockage de documents en local sur son poste de travail, et privilégier l'utilisation des répertoires réseaux mis à disposition.

Seuls les lecteurs réseaux sont sauvegardés. Les fichiers enregistrés en local (sur le disque de l'ordinateur) ne pourront pas être récupérés en cas de perte.

Les données professionnelles doivent être sauvegardées sur les ressources partagées adéquates de la Commune et non détruites – non effacées par l'*Utilisateur* lors de son départ.

Point d'attention :
Il est possible de télécharger tous documents ou informations sur son disque local, mais le stockage de ces données doit se faire de manière temporaire. Il faut penser à transférer ces données du disque dur local sur un des lecteurs réseaux adaptés à son contexte ou à les supprimer.

5.4.6. Règles relatives aux solutions Cloud

La souscription ou l'usage de ce type de service dans le cadre de l'activité professionnelle, sans validation préalable du service informatique et hors des solutions approuvées par le service informatique, est strictement interdite.

Dans tous les cas, la présente charte **s'applique dans son intégralité** sur le périmètre des services de « Cloud computing » quels qu'ils soient.

5.4.7. Règles relatives aux mises à jour système et sécurité

Pour installer les nouveaux correctifs et les différentes mises à jour, le service informatique réalise des mises à jour régulières. L'*Utilisateur* doit laisser faire ces mises à jour sans aucun blocage (tous les jours sinon au minimum 1 fois/semaine).

Les mises à jour à effectuer sont imposées par le service informatique.

5.5. Internet

La Commune de Saint-Louis met à disposition de ses *Utilisateurs* un accès Internet destiné à un usage professionnel. Il est paramétré et administré à cet effet.

5.5.1. Règles relatives à la sécurité des moyens de connexion

L'*Utilisateur* doit obligatoirement utiliser en l'état les moyens de connexion à Internet fournis par la Commune de Saint-Louis. A ce titre, l'*Utilisateur* s'interdit de modifier les paramètres de

sécurité ou de contourner les restrictions mises en place, et utilise impérativement les navigateurs Internet installés par le service informatique de la Commune.

Dans le cas d'une connexion hors des locaux de la Commune, l'*Utilisateur* privilégie l'utilisation des moyens mis à disposition par la Commune (Cf. **5.9 Règles relatives à l'utilisation des équipements en situation de mobilité**).

5.5.2. Règles relatives à l'utilisation de l'accès Internet

L'*Utilisateur* s'engage à ne pas utiliser l'accès Internet mis à disposition par la Commune de Saint-Louis pour toute activité (consultation de site, transmission / téléchargement de documents, etc.) comportant des éléments manifestement illicites ou pouvant heurter la sensibilité d'une autre personne.

L'*Utilisateur* s'engage à respecter les conditions d'utilisation des sites visités.

L'*Utilisateur* doit impérativement limiter au strict nécessaire toute activité engendrant un large trafic (téléchargements volumineux, radios en ligne, vidéos en ligne, etc.).

La Commune se réserve le droit, pour des impératifs de sécurité, de disponibilité et de performance des ressources, de filtrer, limiter et contrôler l'accès Internet fourni aux *Utilisateurs*. L'*Utilisateur* peut adresser au service informatique une demande, motivée par une justification professionnelle, de levée partielle de ces mesures.

5.5.3. Règles de nétiquette et manière de s'exprimer en public

L'*Utilisateur* ne doit pas publier d'information concernant la Commune de Saint-Louis ou son activité sur les blogs ou réseaux sociaux, sauf si une telle publication est faite dans le cadre de l'exécution de sa mission, et dans la limite de son domaine de responsabilités.

À ce titre, il est notamment interdit de communiquer de manière directe ou indirecte sur des projets internes de la Commune Saint-Louis avec ses comptes privés sur les réseaux sociaux.

Dans ce cadre, l'*Utilisateur* doit faire preuve d'une grande vigilance sur les informations communiquées, et notamment doit les communiquer avec soin et courtoisie, afin de s'assurer que leur communication ne soit pas, directement ou indirectement, préjudiciable aux intérêts et à la réputation de la Commune.

L'*Utilisateur* doit s'interdire d'usurper ou d'emprunter l'identité d'un tiers, et utilise impérativement son identité propre pour les échanges professionnels, notamment sur les blogs ou réseaux sociaux.

5.6. Terminaux mobiles

5.6.1. Règles relatives aux ordinateurs portables

Les *Utilisateurs* disposant d'un ordinateur portable fourni par la Commune de Saint-Louis sont responsables de leur équipement et sont soumis aux mêmes règles d'utilisation que celles applicables aux postes de travail fixes.

Les ordinateurs portables non connectés au réseau, surtout la nuit, doivent être rangés dans une armoire ou un tiroir, si possible fermés à clé, lorsqu'ils ne sont pas utilisés.

L'*Utilisateur* doit s'assurer que tout travail effectué à distance est enregistré sur les systèmes de la Commune. Seules les données nécessaires lors des déplacements doivent être stockées sur le disque dur de l'ordinateur portable.

En outre, lors de ses déplacements, l'*Utilisateur* doit veiller à ne pas laisser son équipement mobile sans surveillance (hôtel, voiture, train, etc.)

5.6.2. Règles relatives à l'utilisation de supports amovibles

Il est, en principe et sauf dans les cas explicitement autorisés par le service informatique, interdit aux *Utilisateurs* de stocker des données sur des supports amovibles.

L'*Utilisateur* doit éviter, lorsque cela est possible, la connexion de supports amovibles sur son poste de travail, en privilégiant l'utilisation de solutions de transfert de données mises à disposition par la Commune de Saint-Louis. Lorsque cela est strictement nécessaire pour répondre à un besoin professionnel de transfert ponctuel de données l'*Utilisateur* doit s'assurer que le support utilisé ne contient pas de virus (avec éventuellement l'aide du service informatique).

L'*Utilisateur* ne doit en aucun cas connecter un support amovible confié par une personne inconnue ou offert par un tiers (ex. « goodies », clé USB ou tout autre support / gadget offert ou acheté).

L'*Utilisateur* prend le soin de supprimer de manière sécurisée les données qui transitent sur des supports amovibles à des fins de transfert.

Le service informatique de la Commune se réserve le droit de bloquer l'usage de supports amovibles.

5.6.3. Règles relatives aux smartphones professionnels

La Commune de Saint-Louis met à la disposition de ses *Utilisateurs* des smartphones (tels que : les iPhones et les Android) pour les besoins de leur activité. L'utilisation de ces smartphones implique l'acceptation des règles énoncées dans la présente charte.

Le smartphone et sa carte SIM sont la propriété de la Commune de Saint-Louis et doivent lui être rendus à la fin de la mission de l'*Utilisateur.*

L'utilisation des ressources à des fins privées est tolérée de manière occasionnelle (Cf. **5.2 Tolérance de l'utilisation à des fins privées**).

Les mêmes règles de sécurité s'appliquent aux postes de travail fixes et aux appareils mobiles. Les bonnes pratiques de sécurité spécifiques aux smartphones sont les suivantes :

- Le smartphone est nominatif et ne doit pas être prêté à un tiers (sauf exceptions avec autorisation formelle du service informatique, notamment en cas d'astreintes). Dans le cas contraire, l'Utilisateur sera considéré comme responsable de toute opération devant être effectuée à partir dudit smartphone par ce tiers ;
- Pour protéger la confidentialité des données, l'Utilisateur doit régler son appareil sans fil de manière à entrer un mot de passe pour le déverrouiller. De plus, l'appareil doit être configuré pour se verrouiller automatiquement après quelques minutes ;
- Il est interdit d'effectuer toute opération visant à obtenir des droits administratifs ou de « jailbreaker » ledit smartphone ;
- Il est toléré d'installer des applications non professionnelles sur les smartphones si et seulement si elles sont installées depuis un store officiel et que leur utilisation respecte les règles fixées au 5.2 Tolérance de l'utilisation à des fins privées. En effet, certaines applications peuvent contenir des logiciels malveillants qui peuvent accéder à tout le contenu de vos appareils mobiles (courrier électronique, SMS, documents, photos, applications bancaires, etc.) ;
- Choisir des connexions en données mobiles plutôt que des connexions Wifi tout en restant vigilant sur les coûts de connexion à l'étranger ;
- Désactiver les connexions Wifi ou Bluetooth lorsqu'elles ne sont pas utilisées.

5.6.4. Règles relatives à la protection physique (vol/perte) des terminaux mobiles

L'*Utilisateur* doit adopter un comportement responsable pour limiter les risques de casse, perte ou de vol de ses terminaux mobiles, notamment en maintenant une surveillance constante

dans les lieux publics (Cf. **5.9 Règles relatives à l'utilisation des équipements en situation de mobilité**).

L'*Utilisateur* s'engage à contacter sans délai le service informatique en cas de casse, perte ou vol d'un équipement informatique ou téléphonique afin que ce dernier prenne toutes les mesures de sécurité nécessaires. Ces mesures peuvent comprendre la réinitialisation du terminal à distance et/ou sa déconnexion du système d'information de la Commune et la réinstallation des mots de passe.

En cas de vol, l'*Utilisateur* doit, dans la mesure du possible changer tous les mots de passe, en particulier ceux concernant la messagerie électronique, les comptes de connexion à distance (VPN, etc.) et les sites web (idéalement, il faut aussi changer les questions de vérification des comptes).

En parallèle, l'*Utilisateur* doit dans les meilleurs délais déclarer la perte ou déposer une plainte en cas de vol auprès d'un service de police nationale ou de gendarmerie nationale du lieu du vol (pays, ville) et garder une copie de la déclaration (mentionnant la date, l'heure et le lieu du vol), puis envoyer une copie de cette plainte au service des ressources humaines ou service informatique de la Commune.

5.7. Messageries

La Commune de Saint-Louis met à disposition de ses *Utilisateurs* une messagerie électronique, et le cas échéant une messagerie instantanée, destinées à un usage professionnel. Ces services sont paramétrés et administrés à cet effet.

Un usage, à titre privé, des services de messageries mis à disposition par la Commune est toléré dans les limites définies au chapitre **5.2 Tolérance de l'utilisation à des fins privées**. Des principes de secret des correspondances et de respect de la vie privée nécessite que l'*Utilisateur* respecte les règles suivantes : la mention « Privé » ou « Perso » ou « Personnel » doit systématiquement figurer au début de l'objet du message, le tiers destinataire doit être informé de cet usage, toute signature identifiant la Commune de Saint-Louis (notamment en fin de message) doit être supprimée et enfin les messages privés doivent être rangés dans un répertoire dédié de la messagerie portant la mention « Privé » ou « Perso » ou « Personnel ».

5.7.1. Règles relatives à la sécurité des services de messageries

L'*Utilisateur* doit obligatoirement utiliser en l'état les services de messagerie installés et configurés par la Commune. A ce titre, l'*Utilisateur* s'interdit de modifier les paramètres de sécurité.

L'*Utilisateur* s'engage à ne pas utiliser, pour ses usages professionnels, des services de messagerie ou de partage / stockage de données autres que ceux mis à disposition par la Commune (ex. une messagerie personnelle Gmail, Yahoo, etc., un service de stockage cloud non maîtrisé par la Commune, Dropbox, etc., un service de transfert de fichiers WeTransfer, etc.).

L'*Utilisateur* s'interdit de transférer des messages professionnels vers sa messagerie personnelle.

5.7.2. Règles relatives à l'usage des services messageries

L'*Utilisateur* s'attache à libeller explicitement l'objet du message, soigner sa rédaction et son contenu ainsi que le choix des destinataires des messages.

- L'*Utilisateur* s'engage à respecter et utiliser les « en-têtes » dans les mails :

- Pour information ;
- Pour action ;
- Pour avis.

L'*Utilisateur* s'engage à saisir sa signature professionnelle dans tous ses e-mails professionnels.

L'*Utilisateur* s'attache à faire attention aux choix des destinataires et des personnes à mettre en copie.

L'*Utilisateur* s'engage à ne pas utiliser les services de messagerie mis à disposition pour envoyer ou faire suivre des messages comportant des éléments manifestement illicites ou pouvant heurter la sensibilité d'une autre personne.

La Commune se réserve le droit, pour des impératifs de sécurité, de disponibilité et de performance des ressources, de limiter la taille maximum des messages, des boîtes aux lettres et de certains types de fichiers attachés. L'*Utilisateur* peut adresser au service informatique une demande, motivée par une justification professionnelle, de levée partielle de ces mesures.

5.7.3. Règles relatives à la protection contre l'hameçonnage et la fraude

L'*Utilisateur* doit éviter, autant que faire se peut, de publier son adresse électronique sur Internet (ex. publication sur des blogs ou des profils de réseaux sociaux).

L'*Utilisateur* doit faire preuve d'une vigilance accrue en cas de réception d'un message inhabituel ou douteux en provenance d'un expéditeur inconnu, présentant une syntaxe approximative, contenant des liens vers des sites et/ou des pièces jointes non sollicités, ou demandant d'effectuer des actions inhabituelles. Lorsque l'*Utilisateur* pense avoir reçu un tel message, il n'y répond pas et le signale immédiatement au service informatique, sans tenter d'accéder aux liens contenus dans le message ou d'ouvrir les pièces jointes associées.

L'*Utilisateur* ne doit cliquer sur un lien hypertexte contenu dans un message que lorsqu'il estime avoir « toute confiance » dans l'expéditeur et seulement après avoir vérifié la syntaxe du lien hypertexte. Si ce lien le dirige sur un site qui lui demande une authentification, l'*Utilisateur* doit redoubler de vigilance, et contrôler l'adresse « réelle » du site cible avant de saisir ses identifiants et mot de passe. Si l'*Utilisateur* a le moindre doute, il doit contacter sans délai le service informatique.

En raison des risques d'usurpation d'une adresse de messagerie, l'*Utilisateur* doit faire preuve de discernement en cas de réception d'un message électronique « a priori » en provenance d'un responsable ou d'un tiers connu, lui demandant d'effectuer des actions inhabituelles ou non-conformes aux procédures internes. Dans ce cas, l'*Utilisateur* doit vérifier verbalement auprès de cette personne le bien-fondé de l'action (appel téléphonique, échange dans son bureau, etc.).

5.7.4. Règles relatives à l'envoi de données sensibles par messagerie

Il convient de rappeler qu'il est impossible de garantir la confidentialité des échanges par messagerie. En conséquence, il convient d'éviter d'échanger des ***informations sensibles*** par messagerie. Quand il n'est pas possible de faire autrement, l'*Utilisateur* doit prendre le soin de limiter l'envoie d'***informations sensibles*** aux seules personnes ayant besoin d'en disposer dans le cadre de leur activité. En retour, l'*Utilisateur* qui reçoit des ***informations sensibles*** s'interdit de faire suivre le message, seul l'émetteur à l'origine du message décidant de la liste de diffusion.

L'*Utilisateur* peut également chiffrer le fichier joint avec un mot de passe.

Envoyé en préfecture le 06/11/2024
Reçu en préfecture le 06/11/2024
Publié le
ID : 974-219740149-20241029-DCM134_2024-DE

5.8. Imprimante, photocopieuse et broyeur.

L'*Utilisateur* doit être vigilant de la même manière sur l'utilisation des imprimantes, des photocopieurs et des broyeurs que pour les postes de travail informatique et autres outils.

Point d'attention :
Il convient d'avoir une vigilance accrue des *Utilisateurs* pour éviter de laisser tous documents sensibles dans le bac des imprimantes et du broyeur.
De plus, il convient d'utiliser les broyeurs pour détruire tous les supports contenant des données à caractère personnel et/ou confidentielles.

5.9. Règles relatives à l'utilisation des équipements en situation de mobilité

L'*Utilisateur* adopte les bons comportements pour limiter le risque de perte ou de vol de ses équipements en dehors des locaux de la Commune (transports en commun, hôtels / restaurants, sites professionnels tiers, domicile, etc.).

L'utilisation de téléphones mobiles, d'ordinateurs portables et d'assistants personnels a facilité le transport et l'échange de données. Certaines de ces informations peuvent être très sensibles. Leur perte, saisie ou vol peut avoir un impact important sur la Commune et sa pérennité. Elles doivent être protégées contre les risques et les menaces auxquels elles sont confrontées, en particulier lors de déplacements. Les bonnes pratiques de sécurité spécifiques à la mobilité sont les suivantes :

- L'Utilisateur prend soin de ne jamais stocker d'informations stratégique sur des équipements portables non chiffrés ;
- Privilégier le stockage réseau via l'accès VPN et/ou le Drive ;
- Suppression des fichiers locaux non nécessaires à la mission ;
- L'Utilisateur active les connexions Wifi ou Bluetooth de ses équipements uniquement lorsque celles-ci sont absolument nécessaires :
    - Pour les ordinateurs portables, l'Utilisateur doit systématiquement utiliser une connexion réseau à distance sécurisée (VPN), mise à sa disposition par le service informatique ;
    - Pour les smartphones, l'Utilisateur doit utiliser les points d'accès Wifi publics, si et seulement si, il ne peut pas utiliser les données mobiles.
- L'Utilisateur ne doit pas connecter son équipement à des ordinateurs ou des périphériques informatiques non fiables ;

5.10. Applications, serveurs internes

L'accès aux applications et aux serveurs internes est mis à disposition des *Utilisateurs* pour un usage professionnel. Il est paramétré et administré à cet effet. Pour des raisons de performance et de maîtrise du réseau, l'usage à titre privé de ces ressources n'est pas autorisé.

5.10.1. Règles relatives au téléchargement et installation des applications

Le poste de travail informatique est équipé de logiciels sélectionnés par la Commune, pour leur compatibilité entre eux et leur capacité à répondre aux besoins de chaque *Utilisateur* dans l'exercice de ses fonctions, et pour lesquels la Commune paie une licence d'utilisation.

Pour ces raisons, les *Utilisateurs* ne sont pas autorisés à sauvegarder, installer, importer ou modifier des logiciels sur leur poste de travail. Seul le service informatique est autorisé à effectuer ces actions sur les postes de travail.

Le téléchargement de logiciels ou de nouvelles versions de logiciels sur Internet, ou de toute autre source, à l'initiative de l'*Utilisateur*, est interdit, même s'il s'agit de logiciels libres.

Le téléchargement de logiciels antivirus est particulièrement interdit. Le service informatique veille à ce qu'un logiciel anti-virus soit installé sur chaque poste de travail et serveur du réseau et à ce qu'il soit actif. L'*Utilisateur* ne doit en aucun cas les désactiver ou modifier leur configuration.

L'*Utilisateur* ne doit pas détruire, modifier les données ou accéder aux informations appartenant à d'autres *Utilisateurs* sans leur autorisation. Il ne doit pas non plus tenter d'accéder à des zones interdites du réseau.

En outre, les *Utilisateurs* ne sont autorisés à importer, envoyer ou distribuer des fichiers qu'à la condition que ces opérations soient effectuées dans le cadre de leur activité professionnelle.

L'utilisation des ressources à des fins privées est tolérée de manière occasionnelle (Cf**. 5.2 Tolérance de l'utilisation à des fins privées**).

5.11. Contrôle des ressources

Conformément à la loi, la Commune de Saint-Louis est responsable de l'utilisation faite par les *Utilisateurs* des ressources du système d'information mises à leur disposition. La Commune se réserve ainsi le droit d'analyser, de limiter et de contrôler l'utilisation des ressources matérielles et logicielles ainsi que les échanges effectués via son système d'information.

5.11.1. Objets et encadrement des contrôles réalisés par la Commune

Les contrôles sont réalisés par les administrateurs du service informatique dans l'objectif de garantir le bon fonctionnement technique et la sécurité du système d'information, et de préserver les intérêts de la Commune.

Les contrôles sont réalisés exclusivement par les membres habilités du service informatique de la Commune qui garderont confidentielles les informations qu'ils pourraient être amenés à connaître à cette occasion.

5.11.2. Opérations récurrentes de contrôle sur les journaux d'événements

La Commune met en œuvre différents dispositifs de contrôle de l'utilisation des ressources du système d'information. Ces dispositifs génèrent des journaux conservant les traces de certaines actions des *Utilisateur*s. Le service informatique réalise des opérations récurrentes de contrôle portant sur ces journaux.

5.11.3. Opérations ponctuelles de contrôle sur les données

La Commune peut à tout moment et en dehors de la présence des *Utilisateur*s, opérer tout contrôle sur les données présumées à caractère professionnel, qu'il s'agisse par exemple de la messagerie électronique ou des fichiers enregistrés. L'accès aux données est réalisé par les membres habilités du service informatique de la Commune.

Dans le cas de fichiers identifiés comme étant de nature privée conformément aux règles précisées dans la présente charte, les administrateurs informatiques chargés des opérations de contrôle peuvent néanmoins procéder à des contrôles sur la taille et le volume, et ce sans accéder aux contenus. La Commune ne peut accéder à ces données qu'en présence de l'*Utilisateur* ou lorsque celui-ci a été dûment invité à être présent par tout moyen approprié.

En cas de risque ou évènement particulier présentant à la fois un caractère d'urgence et de gravité certain, la Commune peut néanmoins accéder aux fichiers identifiés comme étant de nature privée sans la présence ou la convocation de l'*Utilisateur*.

5.11.4. Actions à la suite des contrôles

Dans le cas de circonstances graves d'utilisations illégales ou non autorisées ou remettant en cause le bon fonctionnement du système d'information, la sécurité ou les intérêts de la Commune de Saint-Louis, les membres du service informatique pourront mettre en œuvre les actions de protection adaptées et/ou de corrections nécessaires jusqu'au retour à la normale, et informer la Direction.

5.12. Fin de contrat d'un *Utilisateur*

Tout *Utilisateur* quittant son poste à la Commune de Saint-Louis s'engage à remettre en mains propres, au service informatique l'ensemble des équipements qui a été mis à sa disposition pour l'exercice de sa fonction. Le service informatique procédera ensuite à la désactivation de son compte afin de le protéger d'un quelconque usage malveillant résultant d'un accès illicite à ses données confidentielles.

Lors du départ d'un *Utilisateur,* c'est à lui et lui seul de supprimer ses données privées de son poste et de la messagerie. Le service informatique n'est pas garant des données privées et donc ne pourra pas les récupérer et/ou les restituer.

5.13. Législation et règlements

5.13.1. Propriété intellectuelle

L'*Utilisateur* s'engage à ne pas utiliser l'accès internet et les ressources de la Commune mis à sa disposition à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin – tels que des textes, images, logos, dessins, photographies, œuvres musicales, œuvres audiovisuelles, logiciels et jeux vidéo, et/ou par tout droit de propriété industrielle – sans autorisation tacite.

Ces actes peuvent donner lieu à l'application de sanctions pénales pour contrefaçon.

Le fait qu'un contenu, document, une photo ou un article soit publié en ligne ne signifie pas que ce contenu est libre de droits.

5.13.2. Traitement de données à caractère personnel

5.13.2.1. Responsabilité et devoirs des *Utilisateurs*

Un *Utilisateur* qui accède à ou reçoit des données à caractère personnel, qu'il s'agisse de données relatives aux collaborateurs de la Commune ou à des tiers (clients, partenaires, candidats, etc.), s'engage à respecter strictement la réglementation applicable et les consignes associées au traitement de ces données selon les lois nationales en vigueur.

Plus précisément :

Les traitements de données à caractère personnel sont soumis au RGPD et doivent respecter ce dernier et plus particulièrement les principes suivants :

1. Traiter les données de manière licite, loyale et transparent : il convient de fournir toute information en ce qui concerne le traitement de données à caractère personnel à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, et en des termes clairs et simples.

2. Avoir des finalités déterminées : les données doivent être collectées et traitées pour des finalités déterminées, explicites et légitimes (par exemple : gestion d'une commande, procéder à un recrutement, envoie de newsletter, etc.). Ces données ne doivent pas être réutilisées pour des finalités autres.
3. Minimiser la récolte des données : les données collectées doivent être pertinentes, adéquates et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont collectées et traitées. De même, l'*Utilisateur* ne doit pas avoir accès, ou chercher à avoir accès à des données à caractère personnel qui ne sont pas nécessaires à sa mission.
4. Récolter des données exactes : les données doivent être exactes et, si nécessaire, mises à jour.
5. Limiter la conversation des données : les données doivent être conservées pour la période strictement nécessaire à l'accomplissement de la finalité poursuivie. A ce titre, l'*Utilisateur* s'engage à respecter les instructions en matière de durée de conservation.
6. Garantir l'intégrité et la confidentialité des données : les données doivent être traitées de façon à garantir leur sécurité à l'aide de mesures appropriées (par exemple : protection contre le traitement non-autorisé, la perte, la destruction des données). Ces mesures de sécurité doivent être prises en consultation avec le DPO et le service informatique de la Commune.

Dans tous les cas, si l'*Utilisateur* est victime ou détecte une violation de données à caractère personnel, il devra prévenir son manager ainsi que le Data Protection Officier (« DPO ») de la Commune de Saint-Louis à l'adresse : dpo@saintlouis.re

5.13.2.2.Droits des Utilisateurs

Les *Utilisateurs* dont le traitement des données à caractère personnel est soumis au RGPD sont informés qu'ils disposent d'un droit d'accès et de rectification relatif à l'ensemble de leurs données à caractère personnel les concernant, d'un droit d'opposition pour motif légitime, d'un droit d'effacement, de limitation du traitement ou encore un droit à la portabilité de ces données. L'*Utilisateur* peut exercer ses droits en contactant le DPO désigné par la Commune.
Violation de la charte

Toute violation de la charte expose l'*Utilisateur* à des sanctions disciplinaires, pénales et/ou civiles, avec des répercussions sur le lien contractuel qui l'unit à la Commune de Saint-Louis.

En outre, la Commune se réserve le droit de mettre fin à tout acte qui est à l'origine de la violation de la charte dans les respects des lois en vigueur.

6. Entrée en vigueur – distribution – modification de la charte

Cette charte a été rédigée par le service informatique de la Commune de Saint-Louis. Elle est applicable à partir du XX/XX/2024.

Elle est distribuée à l'ensemble du personnel. Une version papier est disponible pour tous les *Utilisateurs* sur demande à leurs supérieurs.

Elle sera susceptible d'être modifiée, notamment pour tenir compte de l'évolution constante des contraintes réglementaires et des techniques informatiques ; les utilisateurs seront informés de la publication de nouvelles versions et de la nature des changements apportés.

Envoyé en préfecture le 06/11/2024
Reçu en préfecture le 06/11/2024
Publié le
ID : 974-219740149-20241029-DCM134_2024-DE

Fait à : …… ……., le : ……

Signature