VILLE DE SCEAUX
À LA CROISÉE DES TALENTS

Charte d'utilisation des Systèmes d'Information

Adopté lors de la séance du conseil municipal du 24 mars 2022

Annexe au règlement intérieur de l'administration de la ville de Sceaux

SOMMAIRE

Préambule

La ville de Sceaux a mis en place un système d'information et de communication nécessaire à ses activités comprenant notamment un réseau informatique et téléphonique et des outils mobiles. Les utilisateurs, dans l'exercice de leurs fonctions, sont amenés à utiliser les outils informatiques et téléphoniques mis à leur disposition. Dans ce cadre, ils s'engagent à respecter les règles de la présente charte d'utilisation des systèmes d'information.

La charte est annexée au règlement intérieur de la ville de Sceaux, pour que chaque agent en ait connaissance.

Ce document a fait l'objet d'un avis du comité technique en date du 14 mars 2022 a été soumis au conseil municipal lors de sa séance du 24 mars 2022.

Cette charte pourra être complétée ou modifiée par la ville de Sceaux. Toute modification sera notifiée aux agents via le compte-rendu du comité technique (joint aux fiches de paie).

La présente charte est applicable à compter de son adoption par le conseil municipal.

Article 1. Champ d'application

La présente charte s'applique à **l'ensemble des utilisateurs** du système d'information (S.I) de la ville de Sceaux, et notamment :

- Les élus
- Les agents municipaux (titulaires ou contractuels, stagiaires)
- Les vacataires
- Les stagiaires, apprentis ou équivalents
- Les intérimaires
- Les employés de sociétés prestataires
- Les visiteurs occasionnels qui seraient amenés à utiliser les outils S.I de la Ville, notamment les agents d'autres collectivités venant en formation à Sceaux.

Il appartient à chaque utilisateur de ne pas permettre l'accès au S.I à des tiers non autorisés.

Article 2. Composition du « Système d'Information » (S.I.)

Le S.I. est composé des ressources et équipements suivants :

- Postes de travail (ordinateur fixe ou portable)
- Téléphones (fixe ou portable)
- Tablettes et smartphones
- Supports de stockage (clé USB, disque dur externe…)
- Câbles divers (Ethernet, HDMI, VGA…)
- Réseau informatique (routeurs, switchs, connectique filaire et Wi-Fi)
- Imprimantes, scanners, multi-fonctions
- Serveurs d'administration et serveurs hébergeant les logiciels métiers et les fichiers
- Données numériques
- Logiciels informatiques (logiciels métier, logiciel de messagerie, logiciels applicatifs…)
- Vidéosurveillance
- Contrôle d'accès et alarmes des bâtiments
- Procédures d'utilisation, d'installation…

Cette liste n'est pas exhaustive, car le S.I est en constante évolution, des éléments pouvant s'y ajouter ou être supprimés à tout moment.

Article 3. Règles générales d'utilisation

Le S.I. doit être utilisé à des fins professionnelles, conformes aux objectifs de la ville de Sceaux. A titre exceptionnel, dans des cas prévus par la présente charte ou par la loi, ils peuvent être accessoirement utilisés à des fins personnelles.

En tout état de cause, les utilisateurs ne peuvent en aucun cas utiliser le S.I. pour se livrer à des activités susceptibles de porter préjudice à la ville de Sceaux de quelque manière que ce soit.

Le S.S.I. (service des Systèmes d'information) de la ville de Sceaux met en œuvre une série de moyens pour assurer la sécurité de son S.I. et des données traitées, en particulier des données personnelles. À ce titre, il peut limiter l'accès à certaines ressources.

3.1. Principe général de responsabilité et obligation de prudence

L'utilisateur est responsable des ressources informatiques qui lui sont confiées dans le cadre de ses missions et doit concourir à leur protection, notamment en faisant preuve de prudence. L'utilisateur doit s'assurer d'utiliser les ressources informatiques mises à sa disposition de manière raisonnable, conformément à ses missions.

Article 3.2. Obligation générale de confidentialité

L'utilisateur s'engage à préserver la confidentialité des informations et en particulier des données personnelles, traitées sur le S.I. Pour plus de précision, voir l'engagement de confidentialité en annexe 1.

Il s'engage à prendre toutes les précautions utiles pour éviter que ne soient divulguées de son fait, ou du fait de personnes dont il a la responsabilité, ces informations confidentielles (personnelles, bancaires ou administratives).

3.3. Mot de passe

L'accès au S.I. ou aux ressources informatiques mises à disposition est protégé par un mot de passe individuel. Le login (identifiant personnel) et le mot de passe doivent être saisis lors de chaque accès au S.I.

Ce mot de passe doit être gardé confidentiel par l'utilisateur afin de permettre le contrôle de l'activité de chacun. Le mot de passe doit être mémorisé et ne doit pas être écrit sur un fichier informatique ni sur un support facilement accessible par un tiers.

Il ne doit pas être transmis ou confié à un tiers ou être rendu accessible, même sur demande de la hiérarchie.

Pour plus de précision sur la composition du mot de passe, voir la politique des mots de passe pour les accès au S.I. en annexe 2.

3.4. Verrouillage de sa session

En cas d'absence, même temporaire (quelques minutes), il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

Pour mémoire, le poste se verrouille par la combinaison des touches suivantes :  .

3.5. Installation de logiciels (PC, Smartphone et tablette)

L'utilisateur a interdiction d'installer des logiciels, de copier ou télécharger des fichiers susceptibles de créer des risques de vulnérabilité au sein de la ville de Sceaux.

Il doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle et le secret professionnel. Il est notamment strictement interdit de télécharger des films venant de plateformes de type peer-to-peer.

L'utilisateur est responsable des équipements qui lui ont été confiés et ne pourra pas arguer d'une non-compétence en informatique pour se dédouaner de l'installation d'un programme ou logiciel non autorisé sur son poste de travail, smartphone ou tablette.

L'utilisateur ayant besoin d'un nouveau logiciel ou application peut faire une demande au S.S.I. pour l'installation de logiciels libres de droit « open source » ou de logiciels sous licence ayant fait l'objet d'une acquisition officielle par la ville de Sceaux.

Tout logiciel installé illicitement ou tout fichier suspect sera supprimé par le S.S.I. dès le constat de leur présence sur le poste de travail. Cette installation frauduleuse ou non conforme pourra faire l'objet d'une sanction disciplinaire.

L'installation par l'utilisateur ou la simple copie sur un ordinateur d'un programme ayant les propriétés ci-dessous est interdite (liste non exhaustive) :

- programmes d'espionnage d'autres utilisateurs,
- programmes permettant de contourner la sécurité,
- programmes saturant les ressources,
- programmes de type virus et cheval de Troie,
- programmes contournant les protections des logiciels,
- programmes de téléchargement Internet de type « peer-to-peer »
- circulation de données chiffrées autres que celles validées par le S.S.I.

3.6. Copie de données informatiques

Conformément à l'engagement de confidentialité (voir annexe 1), l'utilisateur s'engage à limiter toute copie et divulgation d'information numérique à la seule fin d'exécuter ses fonctions.

Article 4. Modalités d'utilisation des ressources informatiques

Le partage des ressources du S.I. par l'ensemble des utilisateurs ayant des besoins souvent différents impose le respect de quelques règles indiqués dans la charte.

4.1. Accès aux matériels en libre-service (Box, Salle de formation, etc…).

La mise à disposition d'un matériel de prêt (notamment pour la tenue d'une réunion) est soumise à une réservation sur le logiciel de réservation et sous réserve de disponibilité du matériel.

Le demandeur vient chercher et restituer le matériel au sein du service aux jours et horaires d'ouverture habituel du service.

Le demandeur en assure la garde et la responsabilité, et doit informer le S.S.I. en cas d'incident (perte, vol, dégradation) puis procéder aux démarches telles que plainte, déclaration de vol/de perte (voir article 6.1).

Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements (ex : changement du mot de passe d'accès au poste).

Le matériel doit être restitué dans le même état qu'au moment du prêt muni de tous les accessoires fournis.

En outre, les équipements informatiques de la ville de Sceaux ne doivent pas être emportés en dehors des sites de la Ville, sauf accord préalable du chef de service du S.I. ou lors de télétravail déclaré et autorisé.

4.2. Boxes et salle de formation

Boxes : la ville de Sceaux dispose de quatre boxes équipés d'ordinateurs dans lesquels sont accueillis les usagers qui veulent effectuer des démarches auprès de la ville de Sceaux. Il est de la responsabilité des agents de la Ville de ne pas donner aux usagers accès aux ordinateurs et de ne pas connecter un matériel quelconque provenant des usagers (clés USB...). Ces connexions de clés USB représentent un vecteur de virus très nocif.

Salle de formation : la ville de Sceaux possède une salle de formation destinée au personnel municipal, équipée d'une dizaine de postes de travail et d'un vidéoprojecteur.

Cette salle peut accueillir les ordinateurs portables des formateurs, mais ceux-ci ne seront pas connectés au réseau interne du S.I.

Lors de formation conjointe avec d'autres entités, les utilisateurs externes devront signer une charte spécifique et un compte utilisateur non nominatif leur sera dédié pendant toute la durée de la formation, afin d'effectuer une traçabilité de leur utilisation du S.I.

4.3. Support de stockage nomade

On entend par « stockage nomade » tous les moyens techniques mobiles qui permettent de stocker des données (ordinateur portable, tablette, téléphones mobiles ou Smartphones, clé USB, disque externe, etc.).

Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, au moyen des solutions suivantes (liste non exhaustive) :

. Ordinateur portable : chiffrage du disque dur (exemple BitLocker)
. Smartphone, Tablette et GVE : code de déverrouillage (4 chiffres / dessin)
. Clé USB et disque externe : mot passe pour les fichiers ou conteneur chiffré (sorte de « valise diplomatique » que seuls les destinataires ont le droit de lire)

4.4. Stockage partagé

Un espace de stockage partagé est mis à la disposition des utilisateurs. Il est accessible à l'adresse suivante : lenuage.sceaux.fr

Cet espace permet de stocker, de mettre à disposition et d'échanger des documents. Il est accessible de n'importe où, dans le respect des règles et modalités précisées dans cette charte. Il est accessible par les utilisateurs ainsi que par des tiers invités.

L'utilisateur peut bénéficier de fonctionnalités de partage et de synchronisation de fichiers. Pour en savoir plus sur l'ensemble des fonctions permises, l'utilisateur pourra trouver les procédures d'utilisation sur l'intranet ou les demander au S.S.I.

4.5. Téléphone fixe, mobile, smartphone, tablette et GVE

La ville de Sceaux met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et/ou mobiles.

L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.

Des restrictions d'utilisation des téléphones (fixes et mobiles) par les agents sont mises en place en tenant compte de leurs missions. À titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

Le S.S.I peut accéder à l'intégralité des numéros appelés depuis les postes fixes ou depuis les téléphones mobiles. Une consultation des appels sera faite notamment en cas d'utilisation anormale, de facture d'un montant inhabituel ou sur demande de la Direction générale, après avoir prévenu l'agent concerné.

Il est rappelé que l'envoi de SMS est réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel.

Les surcoûts pour la ville de Sceaux engendrés par l'utilisation de la téléphonie à des fins personnelles devront être remboursés par les utilisateurs concernés. Il s'agit tout particulièrement des appels de numéros surtaxés et des appels depuis l'étranger ou à destination de l'étranger.

Les équipements mobiles (smartphones, tablettes) permettant d'accéder à la messagerie électronique professionnelle comportent des risques particuliers liés à la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés, même pendant quelques minutes, ils doivent être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

Les équipements mobiles fournis par la ville de Sceaux sont managés dans le cadre d'une gestion de parc mobile spécifique (MDM), encadrant la mise à niveau de leur système d'exploitation et de leurs applications, ainsi que la protection de leurs données.

4.6. Poste de travail

La ville de Sceaux met à disposition de chaque utilisateur concerné un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions (matériel, système d'exploitation, logiciels).

L'utilisateur doit s'abstenir d'installer ou de supprimer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des vulnérabilités au sein du S.I. de la ville de Sceaux.

Il ne doit pas non plus modifier les paramétrages de son poste de travail ou des différents outils mis à sa disposition, ni contourner aucun des systèmes de sécurité mis en œuvre dans la ville de Sceaux.

Lorsqu'il constate une configuration ou un comportement inhabituel de son matériel, il doit alerter le S.S.I. aussi rapidement que possible.

À des fins de maintenance informatique et d'aide aux utilisateurs, le S.S.I. peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur.

Le BYOD (« Bring Your Own Device ») correspond à un nouvel usage selon lequel les salariés apportent leurs outils personnels (tablette, PC portable, smartphone) et envisagent de les utiliser de manière professionnelle dans leur entreprise. Cette pratique, qui constitue un danger réel pour le S.I. de la ville de Sceaux, est interdite. En revanche, l'usage d'un ordinateur personnel est autorisé dans le cadre du télétravail, dans le respect du protocole sécurisé (VPN) mis en place par le S.S.I.

Toutes les données présentes sur les serveurs de la ville de Sceaux (dossiers partagés, applications et bases de données métiers) sont sauvegardées quotidiennement sous la responsabilité du S.S.I. Dès lors que l'utilisateur stocke ses données sur un autre espace (notamment dossier « Mes Documents », disque dur de l'ordinateur, mémoire du smartphone, etc.), les sauvegardes de ces données ne sont pas assurées par le S.S.I. ; elles sont sous la responsabilité de l'utilisateur. En cas de défaillance de l'équipement, ces données seront perdues, sauf si l'utilisateur en a fait une sauvegarde sur un autre support.

Pour bénéficier des sauvegardes régulières, il est fortement recommandé aux utilisateurs de stocker les fichiers importants, et même tous les fichiers à caractère professionnel, dans les dossiers partagés sur le réseau (répertoire « T »).

4.7. Utilisation des Réseaux et Wi-Fi Pro

Le réseau Wi-Fi (pro) de la ville de Sceaux obéit aux mêmes règles de sécurité que tout le reste du réseau filaire auxquels sont connectés les ordinateurs professionnels.

Certains comportements considérés comme dangereux pour le S.I. de la ville de Sceaux, pourront entraîner la fermeture immédiate du compte utilisateur à titre préventif, afin de protéger le réseau d'une attaque potentielle. Les principaux comportements dangereux sont les suivants :

- interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés
- accéder à des informations privées des autres utilisateurs sur le réseau
- détruire volontairement des informations sur un des systèmes connectés

- mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les matériels dont l'utilisateur à l'usage
- utiliser, même avec leur accord, ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués, ou masquer son identité
- modifier la configuration réseau de son poste de travail informatique

Chaque utilisateur est juridiquement responsable de l'usage qu'il fait de ses connexions. Il s'engage à respecter les règles de déontologie et d'hygiène informatique et notamment :

- ne pas diffuser ses identifiants de connexion (login et/ou mot de passe),
- utiliser les moyens mis à sa disposition conformément aux lois et réglementations en vigueur, en particulier :
  - sans porter atteinte à la vie privée de toute personne ou au secret des correspondances
  - sans intercepter tout message et communication émis par les réseaux
  - sans porter atteinte aux droits d'autrui ou à la sécurité des personnes
- ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :
  - d'altérer, de modifier des données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau
  - d'interrompre ou de perturber le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau
  - de modifier ou de détruire des informations sur un des systèmes
  - de se connecter ou d'essayer de se connecter sur un site sans y être autorisé

L'ensemble des services utilisés génère, à chaque usage, "des fichiers de traces", historique des actions effectuées par les utilisateurs. Ces fichiers conservent des informations : heure de connexion, identifiants de la connexion (adresse IP, adresse MAC de l'ordinateur depuis lequel les services sont utilisés). Ces fichiers sont exploités par le S.S.I. pour l'administration du S.I. Ils servent notamment à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés.

L'article L 34-1 du code des postes et télécommunications électroniques impose la conservation de ces « traces » pendant un an.

Dans le cadre d'une procédure judiciaire, ces fichiers doivent être mis à la disposition de la justice « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ».

Un extrait de ces fichiers sera alors couplé à l'extrait de la base de données des usagers concernés.

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose à la désactivation de son compte d'accès au S.I, ainsi qu'aux poursuites disciplinaires et pénales, prévues par les textes législatifs et réglementaires en vigueur.

4.8. Accès à Internet

Dans le cadre de leur activité, les utilisateurs ont accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le S.S.I. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

La contribution des utilisateurs à des forums de discussion, système de messagerie instantanée, blogs, sites est interdite, sauf autorisation préalable de la Direction générale. Un

tel mode d'expression étant susceptible d'engager la responsabilité de la ville de Sceaux, une vigilance renforcée des utilisateurs est donc indispensable.

L'usage d'applications gratuites hébergés (Doodle, WhatsApp, Signal, Wetransfer, etc…) n'est pas autorisée sur la ville de Sceaux, sauf autorisation préalable de la Direction générale. En effet, ces éditeurs n'ayant pas d'obligation de confidentialité, ils se réservent le droit de détourner ou revendre les données transmises. La divulgation ou fuite de données peut avoir des conséquences sur l'image de la Ville.

L'utilisateur ne doit pas accéder, ni visualiser, ni télécharger des contenus pornographiques, propagande religieuse ou tout autre contenu comportant des images ou commentaires déplacés.

Le téléchargement et la visualisation de fichiers audiovisuels, en général sans rapport avec l'activité professionnelle, provenant de sources suspectes ou inconnues, risque d'introduire des logiciels malveillants et d'endommager le S.I. Par conséquent, l'utilisateur doit s'abstenir de naviguer sur de tels sites, et de télécharger des fichiers, en particulier médias, sans rapport avec l'activité professionnelle ou présentant un risque pour le S.I.

Pour des raisons de sécurité, des mécanismes de filtrage limitant l'accès à certains sites et services en ligne ont été mis en place par le S.S.I. L'utilisateur voulant aller sur ces sites voit son accès refusé. Toutefois, si l'accès à ce site est justifié une demande pourra être formulée au S.I.

4.9. Intranet

Chaque agent a accès à son espace intranet. Pour se faire il dispose de deux méthodes en fonction de l'équipement utilisé.

Si l'agent utilise un ordinateur appartenant à la Ville, il lui faudra saisir son identifiant et son mot de passe seulement.

Si l'agent utilise tout autre équipement, il lui sera alors demandé de renseigner son identifiant et mot de passe, ainsi qu'un mot de passe temporaire qu'il recevra par SMS lors de chaque tentative de connexion depuis un ordinateur hors-mairie.

Afin de pouvoir utiliser son espace intranet, l'utilisateur s'engage à ne pas diffuser à l'extérieur de la mairie, les informations disponibles, de quelques natures que ce soit, au sein de l'intranet. Font l'objet de cette règle, les données de la ville et les données personnelles d'autres agents, les contenus soumis aux droits à la propriété intellectuelle et les photos soumis au droit à l'image notamment.

Si le modérateur de l'intranet estime qu'une publication n'est pas conforme à la loi française, aux bons usages du web ou à cette charte, il se réserve le droit de supprimer le contenu sans préavis.

A noter que la Ville pourra définir des bonnes pratiques d'utilisation de l'intranet, que l'utilisateur devra suivre.

4.10. Email

Chaque agent est doté d'une adresse email (de type : prénom.nom@sceaux.fr) pour l'exercice de ses missions.

Par principe, tous les messages envoyés sont présumés être transmis à titre professionnel.

Par exception, les utilisateurs peuvent utiliser la messagerie à des fins personnelles, dans les limites posées par la loi. Les messages personnels doivent alors porter la mention « privé » ou « personnel » dans l'objet et être classés dans un répertoire « privé » ou « personnel » dans la messagerie. Ils seront alors considérés comme une correspondance privée et protégés à ce titre.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les utilisateurs sont invités à informer le S.S.I. des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

L'utilisation inappropriée ou excessive de l'e-mail est en infraction avec la politique, les normes et pratiques de la ville de Sceaux.

A noter que la ville pourra définir des bonnes pratiques d'utilisation de la messagerie professionnelle, que l'utilisateur devra suivre.

Les mails sont devenus le principal vecteur d'attaque de réseaux informatiques professionnels et personnels. Il convient d'être très vigilant à la réception de mails reçus d'expéditeurs inconnus. Certains messages reçus de tiers externes intègrent des images d'actualités et/ou des liens corrompus sur lesquels l'utilisateur ne doit pas cliquer. En tout état de cause, si l'expéditeur est inconnu, l'utilisateur ne doit surtout pas transférer le message douteux à un collègue, mais le supprimer définitivement, afin d'éviter les dysfonctionnements du S.I, et de ne pas engager la responsabilité civile ou pénale de la ville de Sceaux.

L'utilisateur s'engage à respecter les règles de base suivantes :

- vérifier l'identité de l'expéditeur et faire preuve de méfiance s'il est inconnu
- ne pas ouvrir les pièces jointes des mails reçus de l'extérieur quand l'émetteur du message est inconnu
- détruire les messages du type « chaîne de solidarité »
- ne pas stocker ni faire suivre des gadgets reçus ou trouvés sur Internet
- ne pas faire suivre les messages d'alerte de l'arrivée d'un virus, mais prévenir le responsable du S.S.I

Le contenu de la messagerie électronique de l'utilisateur est conservé sur les serveurs de la ville de Sceaux pendant un an après le départ de celui-ci. Ainsi, ce contenu pourra être mis à la disposition de la justice dans le cadre d'une procédure « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ».

4.11. Accès distant

La ville de Sceaux a mis en place la possibilité de faire du télétravail pour les agents, selon les cas, avec du matériel mis à disposition par la Ville ou du matériel personnel.

Pour prendre connaissance et maintenir des accès distants sécurisés, l'utilisateur se reportera au règlement du télétravail à la ville de Sceaux.

Article 5. Contrôle et collecte d'informations

5.1. Dispositif de contrôle

Pour garantir le bon fonctionnement technique et la sécurité du S.I, la ville de Sceaux se réserve le droit de limiter, d'analyser et de contrôler l'usage des ressources matérielles et logicielles, quelles que soient leur nature ou leur objet et notamment l'usage des postes de travail informatiques, téléphones, accès distants à la messagerie électronique, à Internet et aux fichiers partagés.

Des journaux d'évènements conservent les traces d'utilisation des services, lesquelles traces n'ont pas vocation à surveiller l'activité de façon systématique, mais plutôt à dépanner l'utilisateur en cas de dysfonctionnement ou de comportement anormal détecté, dans un cadre légal et sans jamais nuire à la confidentialité des échanges. La durée de conservation de ces données est d'un an, conformément aux recommandations de la CNIL (Délibération CNIL n°2021-122 du 14 octobre 2021 relative à la journalisation durant six à douze mois).

Des moyens techniques de filtrage d'accès peuvent limiter les possibilités de navigation sur Internet ;
ils ne dégagent pas pour autant l'utilisateur de ses responsabilités.

La messagerie est soumise à des restrictions techniques qui portent sur les volumes des fichiers transmis et sur les extensions de certains fichiers joints.

Des contrôles antivirus et antispam peuvent altérer les contenus de messages suspects, potentiellement porteurs de liens frauduleux ou de fichiers malveillants. La ville de Sceaux ne pourra être tenue pour responsable de la perte de données provoquée par ces contrôles ni des conséquences qui en découleraient.

5.2. Conformité au RGPD et consentement

La ville de Sceaux se conforme à la réglementation européenne RGPD (Règlement général sur la protection des données 2016/679). Par conséquent, les données numériques à caractère personnel sont recueillies pour des finalités prédéterminées, partagées avec des services identifiés et stockées pendant une durée de conservation précisée et acceptée par l'usager lors du recueil de consentement.

Les responsables de traitement précisent sur quelle base légale repose le traitement mis en place. Le consentement de la personne concernée n'est pas obligatoire dans les cas suivants :

- l'exécution d'un contrat ou de mesures précontractuelles
- une obligation légale (recensement de la population par l'INSEE, registre du personnel)
- l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique (fichier de l'administration fiscale…)
- la sauvegarde de l'intérêt vital d'une personne
- l'intérêt légitime (prévention de la fraude, sécurité des réseaux…).

En dehors de ces cas, le recueil préalable et explicite du consentement de la personne concernée est obligatoire.

Les personnes concernées par les données à caractère personnel bénéficient d'un droit à l'information relatif à la collecte des données, d'un droit d'accès et de rectification de leurs données, d'un droit de retrait de consentement et d'une possibilité de s'opposer au traitement pour motif légitime.

Lorsqu'elles considèrent que leurs droits ont été bafoués, elles peuvent demander à la ville de Sceaux de les faire respecter et ont la possibilité d'introduire une réclamation auprès d'une autorité de contrôle telle que la CNIL.

5.3. Arrivée et départ de l'utilisateur

Le chef de service prévient le S.S.I. de l'arrivée du nouvel agent, en complétant sa "fiche d'arrivée". Le S.S.I. crée les codes d'accès et imprime les identifiants Windows sur une fiche remise en main propre au nouvel agent le jour de son arrivée.

Avant tout départ d'un agent, le chef de service doit lui remettre une « fiche de départ ».

L'agent doit se rendre dans chacun des services où il doit rendre du matériel ou des accès (badge, ordinateur portable, téléphone). L'agent doit impérativement faire signer sa feuille de départ à chaque étape pour attester de la bonne restitution des équipements et matériels, avant de la remettre à son supérieur hiérarchique.

5.4. Accès aux informations pour la continuité de service

La continuité des services étant une priorité de la ville de Sceaux, l'agent doit veiller à ce que ses collègues puissent toujours accéder aux documents et dossiers indispensables, par leur mise à disposition dans un dossier partagé ou par envoi électronique.

En cas d'absence prolongée (maladie ou accident), le chef de service peut demander, par écrit, au S.S.I., l'accès à l'espace de travail numérique de l'agent (messagerie, poste de travail, etc.). Le S.S.I. sollicite la validation de la Direction générale et la consultation de la messagerie et des fichiers sera effectuée dans les bureaux du S.S.I. en présence du chef de service demandeur.

Un chef de service peut demander à tout moment de modifier ou supprimer les droits d'accès d'un agent, selon les besoins du service. Sa demande est faite par écrit au S.S.I.

Les droits d'un agent prennent automatiquement fin lors de la cessation de son activité professionnelle au sein de la ville de Sceaux.

5.5. Blocage des accès

En cas de détection d'utilisation illégale ou non autorisée ou pouvant mettre en cause le bon fonctionnement, la sécurité des S.I, ou les intérêts de la ville de Sceaux, le S.S.I. devra mettre en œuvre les actions de protection adaptées et/ou de correction nécessaires jusqu'au retour à la normale, et en informer la hiérarchie.

Les habilitations de l'utilisateur aux ressources informatiques peuvent être modifiées ou retirées à tout moment par le S.S.I, après validation de la Direction générale.

Dès que le S.S.I le jugera nécessaire, pour des raisons techniques ou administratives, les accès à Internet et à la messagerie pourront être suspendus, restreints ou supprimés, individuellement ou collectivement, notamment pour le maintien de la bonne marche ou de l'intégrité du S.I de la ville de Sceaux. Ces dispositions pourront être prises sans information préalable des utilisateurs en cas d'urgence.

Article 6. Comportement en cas d'incident

6.1. Vol, ou perte d'une ressource

En cas de vol ou perte d'équipement informatique (ordinateur, téléphone, smartphone,) fourni par la ville de Sceaux, **l'utilisateur doit informer au plus vite son responsable hiérarchique et le S.S.I.** puis leur communiquer :

- les circonstances de la perte ou du vol, pour permettre à la ville de Sceaux de décider de porter plainte. Attention : l'utilisateur ne doit pas porter plainte en son nom ; seule une personne habilitée peut porter plainte au nom de la ville de Sceaux
- l'inventaire des données qui étaient présentes sur le matériel avec leur niveau de sensibilité et leur niveau de protection au moment de la perte ou du vol

A noter : les équipements mobiles disposent d'un système de géolocalisation qui pourra être activé afin de retrouver le matériel.

Dans le cas où le matériel ne serait pas retrouvé, un blocage de l'IMEI des appareils sera demandé par le S.S.I. aux opérateurs.

Dans le cas où la ville de Sceaux porte plainte, il lui faudra communiquer les adresses MAC du matériel aux autorités compétentes Il faudra donc demander ces informations en amont au S.I.

6.2. Infection ou intrusion sur le poste de travail

En cas de suspicion ou de constatation d'événements pouvant porter atteinte à la sécurité du S.I. de la ville de Sceaux (par exemple, une intrusion ou une infection par un code malveillant sur le poste de travail ou sur des ressources informatiques), l'utilisateur ne doit pas tenter de résoudre lui-même l'incident. L'utilisateur doit :

- éteindre le matériel et le débrancher (électriquement et du réseau informatique)
- prévenir le S.S.I. qui prendra les dispositions nécessaires pour confiner et traiter l'incident

Une infection par un code malveillant (virus, ver, spyware, cheval de Troie, bombe logique, ransomware …) ou une intrusion sur le poste de travail peut se traduire par un comportement anormal du matériel ou des alertes des dispositifs de sécurité (logiciel antiviral, pare-feu local…) ou le chiffrement intempestif de fichiers.

6.3. Dysfonctionnement de l'équipement

En cas de dysfonctionnement du matériel ou de non-respect des exigences précitées, une reconfiguration du système pourra être décidée. Le cas échéant :

- Le S.S.I. réinitialisera l'équipement avec sa configuration initiale standard
- Le S.S.I. ne restaurera pas les données professionnelles stockées sur le matériel ou les données marquées « usage personnel » ; la ville de Sceaux ne pourra être tenue pour responsable de la perte ou de l'altération des données ainsi que des conséquences qui s'ensuivront.

6.4. Respect du matériel

Lors de sa prise de fonction, la mairie fournit du matériel à l'agent, pour l'exercice de ses fonctions. Il est de sa responsabilité de prendre soin du matériel qui lui a été confié.

De ce fait en cas de négligence flagrante ou de destruction volontaire du matériel, des sanctions pourront être prises par la direction à l'encontre de l'agent.

Article 7. Respect des obligations CNIL / RGPD

Si l'utilisateur est amené à constituer un fichier contenant des données à caractère personnel susceptibles de relever de l'application de la loi dite « Informatique et Libertés », l'utilisateur devra en informer le délégué à la protection des données (DPO) de la ville de Sceaux qui est chargé de veiller au respect du RGP.

Les 5 principes clés de la protection des données personnelles sont les suivantes :

- La finalité : les objectifs du traitement respectent les droits et libertés des individus
- La pertinence : ne pas collecter plus de données que ce dont on a vraiment besoin
- La conservation : la durée de conservation doit être définie au préalable
- Les droits : informer les personnes ; obtenir leur consentement ; assurer leur droit d'accéder à leurs données, le droit de les rectifier et le droit de s'opposer à leur utilisation
- La sécurité : prendre toutes les mesures nécessaires pour garantir la sécurité des données (disponibilité, intégrité, confidentialité)

Article 8. Sanctions

Il est rappelé que la présente charte est un document à portée juridique, impliquant des droits et des devoirs pour les utilisateurs.

Tout acte répréhensible commis par un utilisateur est susceptible d'engager la responsabilité civile ou pénale de la ville de Sceaux.

Les manquements aux règles édictées par la présente charte peuvent engager la responsabilité de l'utilisateur et entraîner des sanctions à son encontre (limitation d'usage du S.I., sanctions disciplinaires).

La ville de Sceaux se réserve également le droit d'engager ou de faire engager des poursuites administratives, indépendamment des sanctions disciplinaires mises en œuvre, en cas de fraude informatique, de non-respect des droits d'auteur ou de violation du secret professionnel.

Le chef du S.S.I. peut isoler et conserver les preuves, logs de logiciels, progiciels, programmes, fichiers créés dans le S.I de la ville de Sceaux, dans le cas d'une violation des droits des tiers, de propriété intellectuelle et peut dénoncer tout acte délictueux.

Article 9. Communication

Le S.S.I. est à la disposition des utilisateurs pour leur fournir toute information concernant l'utilisation du S.I. Il informe régulièrement les utilisateurs sur l'évolution des limites techniques du S.I et sur les menaces susceptibles de peser sur sa sécurité.

La présente charte est disponible sur le réseau de la ville de Sceaux et sur l'intranet.

Des opérations de communication, de sensibilisation et de formation internes sont organisées, de manière régulière, afin d'informer les agents sur les pratiques d'utilisation du S.I.

ANNEXE 1 : ENGAGEMENT DE CONFIDENTIALITÉ

Engagement de confidentialité pour les utilisateurs ayant vocation à manipuler des données à caractère personnel

L'utilisateur s'engage, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin de protéger la confidentialité des informations auxquelles il a accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.
L'utilisateur s'engage en particulier à :

- ne pas utiliser les données auxquelles il peut accéder à des fins autres que celles prévues par ses attributions
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales
- ne faire aucune copie de ces données, sauf si ces copies sont nécessaires à l'exécution de ses fonctions
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données
- s'assurer, dans la limite de ses attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données
- en cas de cessation de ses fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données

Cet engagement de confidentialité, en vigueur pendant toute la durée de ses fonctions, demeurera effectif, sans limitation de durée après la cessation de ses fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.
L'utilisateur a été informé que toute violation du présent engagement l'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

ANNEXE 2 : POLITIQUE DES MOTS DE PASSE

La politique de mots de passe de la ville de Sceaux est définie comme suit :

- la longueur minimale du mot de passe doit être de 8 caractères
- le mot de passe doit contenir ces 4 types de caractères :
  - une ou des lettres majuscules
  - une ou des lettres minuscules
  - un ou plusieurs chiffres
  - un ou plusieurs caractères spéciaux parmi les suivants :
    (~! @ # $% ^& * _-+ =' | \ \ (){}\ []:; "' <>,.? /)
- le mot de passe doit être changé tous les 4 mois

ANNEXE 3 : DISPOSITIONS LÉGALES APPLICABLES

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

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

Textes législatifs

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique

Loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public, et diverses dispositions d'ordre administratif, social et fiscal.

Loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle. Elle interdit à l'utilisateur d'un logiciel toute reproduction de celui-ci autre que l'établissement d'une copie de sauvegarde.

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain réprime

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

Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par voie des télécommunications

Loi n°94-361 du 10 mai 1994 portant mise en œuvre de la directive (C. E. E.) n° 91-250 du Conseil des communautés européennes en date du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur et modifiant le code de la propriété intellectuelle**.**

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

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN). Elle est destinée à favoriser le développement du commerce par Internet, en clarifiant les règles pour les consommateurs et les prestataires aussi bien techniques que commerciaux.

Droit disciplinaire

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) pris pour l'application de l'article 136 de la loi du 26 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale et relatif aux agents contractuels de la fonction publique territoriale

Décret n°91-298 du 20 mars 1991 (art. 15) portant dispositions statutaires applicables aux fonctionnaires territoriaux nommés dans des emplois permanents à temps non complet

Code pénal

Code pénal (partie législative) : art 226-16 à 226-24

Code pénal (partie réglementaire) : art R. 625-10 à R. 625-13

Dispositions pénales : art 323-1 à 323-7 du code pénal.

Article 323-1

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.
Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.

Article 323-2

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

Article 323-3

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

Article 323-3-1

Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4

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

Article 323-5

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

1. L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26
2. L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise
3. La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution
4. La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs établissements de l'entreprise ayant servi à commettre les faits incriminés
5. L'exclusion, pour une durée de cinq ans au plus, des marchés publics
6. L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés
7. L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35

Article 323-6

Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39. L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7

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

Réglementation européenne

La convention européenne du 28/01/1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel.

- Elle définit les principes de base de la protection des données que les États doivent concrétiser dans leur ordre juridique interne. Elle exclut en principe les entraves aux flux transfrontières de données entre les parties.
- Elle règle la coopération entre États pour la mise en œuvre de la Convention, en particulier l'assistance qu'un État partie doit prêter aux personnes concernées ayant leur résidence à l'étranger. Enfin, elle met en place un Comité consultatif chargé en particulier de faciliter et d'améliorer son application.

La **directive de la CEE du 21/12/1988** sur l'harmonisation de la protection juridique des logiciels. Elle protège les droits d'auteur, elle interdit en particulier à l'utilisateur d'un logiciel toute reproduction autre que l'établissement d'une copie de sauvegarde.

Le **règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 dit (règlement général sur la protection des données – RGPD)**, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE