SIAAP

Service public de l'assainissement francilien

COMITE TECHNIQUE DU SIAAP

Séance du
MARDI 03 OCTOBRE 2017

PRESENTATION DE LA CHARTE D'UTILISATION DES RESSOURCES INFORMATIQUES ET DE TELECOMMUNICATION ET DE SES DIX POINTS CLE.

POINT SOUMIS POUR AVIS

SIAAP

Service public de l'assainissement francilien

COMITE TECHNIQUE DU SIAAP

Séance du 03 octobre 2017

Présentation de la Charte d'utilisation des ressources informatiques et de communication et de ses dix points clé

Le présent dossier est soumis pour avis

Présentation de la Charte d'utilisation des ressources informatiques et de communication et de ses dix points clé

PREAMBULE

Depuis la première version de la charte d'utilisation des ressources informatiques et de communication, validée en 2004, les nouvelles technologies de l'information et de la communication ont connu une accélération sans précédent. Les gains en puissance ont été importants pour toutes les machines, des équipements mobiles (smart phones et tablettes) sont apparus et de nouveaux services sont proposés.

Ces outils ont pris une place quotidienne importante dans notre travail et notre vie professionnelle, de nombreux médias de communication, avec une rapidité croissante sont désormais disponibles, proposant d'accéder à Internet de n'importe où et n'importe quand. Ces progrès ont généré une plus grande exposition aux « cyber-attaques », il convenait d'encadrer ces nouvelles utilisations pour ne pas dégrader la sécurité des systèmes d'informations.

La charte d'utilisation des ressources informatiques et de communication devait suivre ces évolutions. Un nouveau document a été élaboré, après concertations entre les Correspondants Informatiques, le Service des Affaires Juridiques, la Direction des Ressources Humaines, le Correspondant Informatique et Liberté et un panel d'usagers des systèmes d'information.

Son objectif reste identique : fixer les grandes règles de mise à disposition des ressources informatiques et des moyens de communication ainsi que les droits et devoirs des utilisateurs.

Cependant son périmètre a évolué, pour tenir compte de ces mutations et nouveaux usages.

Le document « La charte informatique en 10 points » permet de s'imprégner rapidement de l'esprit, mais ne dispense en aucun cas d'une lecture complète de la Charte d'utilisation des ressources informatiques et de communication : tout agent se doit de la connaître.

Elle est disponible dans son intégralité dans l'Intranet du SIAAP.

OBJECTIFS

Elle informe des dispositifs de contrôle prévus et est rédigée dans l'intérêt du SIAAP et des utilisateurs des Systèmes d'Information du SIAAP pour une utilisation sécurisée des moyens technologiques mis à disposition.
Elle est basée sur les principes fondamentaux de la Sécurité des Systèmes d'Information.
Elle a pour objectifs :

- de préciser les principaux droits, devoirs et responsabilités des utilisateurs, en accord avec la législation en vigueur et les règles de déontologie ;

- d'informer les agents des dispositifs de contrôle et de surveillance mis en place au SIAAP en lien avec les Systèmes d'Information ;
- de responsabiliser l'utilisateur sur l'usage qu'il fait des ressources du SIAAP mises à sa disposition dans l'exercice de sa fonction ;
- de mettre en évidence la nécessité pour chaque utilisateur de respecter ces règles, pour la sécurité de tous et des Directions du SIAAP.

La charte n'a pas pour objet de couvrir de façon exhaustive tous les cas de figure possibles, mais plutôt de fixer les principes généraux d'utilisation : c'est donc à l'esprit de ces principes que chacun devra s'y référer dans des situations non envisagées.

CHAMPS D'APPLICATION

La charte s'applique aux utilisateurs des ressources informatiques et de communication du SIAAP, quel que soit leur statut interne ou externe.

Le SIAAP s'engage à communiquer et à mettre à disposition la charte à l'ensemble des utilisateurs. Pour les prestataires et partenaires, la charte sera présentée et annexée aux contrats, marchés et conventions.
Réciproquement, tous les utilisateurs s'engagent à connaître et à appliquer les dispositions de la présente charte. Les agents du SIAAP doivent en outre veiller à faire appliquer la charte aux sous-traitants, stagiaires et partenaires du SIAAP dont ils ont la charge.

CE POINT EST SOUMIS POUR AVIS

Annexe 1

Charte informatique

Les dix points clé de la charte informatique

Charte d'utilisation des ressources informatiques et de communication

Version finale du

30/08/2017

Table des matières

1. PREAMBULE

1.1. Objectifs de la charte

La présente charte d'utilisation des ressources informatiques et de communication a pour objet la définition des règles d'accès et d'usage des ressources informatiques et de communication du SIAAP.

Elle informe des dispositifs de contrôle prévus et est rédigée dans l'intérêt du SIAAP et des utilisateurs des Systèmes d'Information du SIAAP pour une utilisation sécurisée des moyens technologiques mis à disposition.

Elle est basée sur les principes fondamentaux de la Sécurité des Systèmes d'Information.

Cette charte a pour objectifs :

- de préciser les principaux droits, devoirs et responsabilités des utilisateurs, en accord avec la législation en vigueur et les règles de déontologie ;
- d'informer les agents des dispositifs de contrôle et de surveillance mis en place au SIAAP en lien avec les Systèmes d'Information ;
- de responsabiliser l'utilisateur sur l'usage qu'il fait des ressources du SIAAP mises à sa disposition dans l'exercice de sa fonction ;
- de mettre en évidence la nécessité pour chaque utilisateur de respecter ces règles, pour la sécurité de tous et des entités du SIAAP.

La charte n'a pas pour objet de couvrir de façon exhaustive tous les cas de figure possibles, mais plutôt de fixer les principes généraux d'utilisation : c'est donc à l'esprit de ces principes que chacun devra s'y référer dans des situations non envisagées.

Elle est disponible dans son intégralité dans l'Intranet du SIAAP.

Les utilisateurs ont, par ailleurs, l'obligation de respecter l'ensemble des lois et réglementations en vigueur, citées à l'article « 5. Législation ».

Les termes visés dans la présente charte font l'objet de définitions à l'article « 6. Définitions ».

1.2. Champ d'application

La charte s'applique à l'ensemble des utilisateurs des Systèmes d'Information du SIAAP dans leur ensemble (de gestion, industriel), quel que soit leur statut et sans que cette liste soit limitative :

- les agents du SIAAP (non- titulaires, titulaires, stagiaires et apprentis, emplois d'avenir)
- le personnel des prestataires,
- les collaborateurs occasionnels et partenaires.

Les Systèmes d'Information sont composés de l'ensemble des ressources informatiques et de communication du SIAAP, à savoir les ordinateurs, serveurs, téléphones (fixes, mobiles et smartphones), logiciels, imprimantes et tout autre matériel connecté aux Systèmes d'Information.

Le SIAAP s'engage à communiquer et à mettre à disposition la charte à l'ensemble des utilisateurs. Pour les prestataires et partenaires, la charte sera présentée et annexée aux contrats, marchés et conventions.

Réciproquement, tous les utilisateurs s'engagent à connaître et à appliquer l'ensemble des dispositions de la présente charte. Les agents du SIAAP doivent en outre veiller à faire appliquer la charte aux sous-traitants, stagiaires et partenaires du SIAAP dont ils ont la charge.

1.3. Principes fondamentaux

1.3.1. Utilisation professionnelle des outils mis à disposition

Les principes fondamentaux de la Sécurité des Systèmes d'Information doivent constituer une ligne directrice pour tous les utilisateurs.

Les utilisateurs sont responsables de l'usage qu'ils font des ressources des Systèmes d'Information.

Le droit d'utilisation des ressources du Système d'Information cesse immédiatement lorsque l'utilisateur quitte le SIAAP ou n'a plus de relation contractuelle avec celui-ci.

Les utilisateurs ne doivent accéder qu'aux informations et ressources nécessaires dans le cadre de leur activité professionnelle.

Tout mécanisme de sécurité ne doit en aucune façon être désactivé ou contourné, même s'il est défaillant.

Les utilisateurs doivent rapidement signaler à leur hiérarchie et à l'assistance informatique les défaillances qu'ils constatent ou suspectent, dans le domaine de la sécurité informatique.

1.3.2. Protection des informations

L'utilisateur veille, en tous lieux et en toutes circonstances, à garantir la protection des intérêts du SIAAP, de son personnel et de ses usagers.

L'utilisateur ne doit consulter, modifier ou supprimer que les données utiles à l'exercice de ses missions. Cela concerne aussi bien les fichiers que les messages électroniques internes ou externes. Il ne doit pas usurper l'identité d'une autre personne et, ce faisant, ne doit pas tenter d'intercepter de communications entre tiers.

2. DROITS ET DEVOIRS DES UTILISATEURS DES SYSTEMES D'INFORMATION

2.1. Utilisation des ressources (équipements et données)

2.1.1. Droit à la déconnexion

En vue d'assurer le respect des temps de repos et de congé, ainsi que la vie personnelle et familiale, la présente charte affirme l'importance d'un usage maîtrisé des ressources informatiques et de communication par l'ensemble des usagers.

Les encadrants ne peuvent pas contacter les agents à moins qu'ils ne soient d'astreinte, en dehors de leurs horaires de travail tels que définis au SIAAP, sauf urgence avérée. Un contact en dehors de ces horaires doit être justifié par la gravité, l'urgence et/ou l'importance du sujet en cause.

L'agent n'est jamais tenu de prendre connaissance des mails ou appels téléphoniques qui lui sont adressés ou d'y répondre en dehors de son temps de travail.

2.1.2. Encadrement de l'usage personnel des Systèmes d'Information

Un usage personnel ponctuel et raisonnable des ressources informatiques et de communication mises à disposition par le SIAAP, dans le cadre des nécessités de la vie courante et familiale, est toléré dès lors qu'il est mesuré, ne porte pas préjudice à l'activité professionnelle et qu'il n'est pas susceptible d'affecter la sécurité, la performance et le bon fonctionnement des Systèmes d'Information ou de mettre en cause l'intérêt et la réputation du SIAAP.

L'utilisateur devra faire apparaître de manière claire le caractère personnel des dossiers, fichiers ou correspondances (mails, SMS) utilisés dans un cadre privé, avec une indication suffisamment visible, y compris les intitulés raccourcis (« personnel », « privé », « PRV », etc.).

Les fichiers ou correspondances qui ne font pas apparaître ce caractère personnel sont présumés avoir un caractère professionnel, de sorte que le SIAAP peut y avoir accès en dehors de la présence de l'agent. Le supérieur hiérarchique, ou toute personne déléguée par ce dernier, est habilité à consulter les fichiers et messages à caractère professionnel.

Avant son départ du SIAAP, il appartient à l'utilisateur de supprimer ses fichiers et messages à objet personnel. Le SIAAP se réserve le droit de supprimer les fichiers après le délai fixé en interne.

2.1.3. Identification / Authentification

Tout accès au Système d'Information effectué grâce à l'identifiant et au mot de passe d'un utilisateur sera réputé réalisé par cet utilisateur sauf en cas avéré d'usurpation d'identité.

Un mot de passe est personnel, confidentiel, incessible.

Chaque utilisateur est seul responsable de la sécurité de son mot de passe. Il lui appartient de le mémoriser et de ne pas le reproduire sur un support écrit accessible à des tiers. Il ne doit en en aucun cas le communiquer à d'autres personnes.

Tout agent doit respecter la politique d'authentification du SIAAP.

Les mots de passe ne sont pas conservés par les équipes en charge de l'exploitation des Systèmes d'Information. En cas de perte, l'utilisateur demandera que son mot de passe soit réinitialisé.

2.1.4. Utilisation du poste de travail

L'accès aux applications SIAAP et aux données associées est soumis à la validation de la hiérarchie. Puis, les équipes en charge de l'exploitation des Systèmes d'Information sont sollicitées pour valider d'un point de vue technique et effectuer l'installation d'une application sur le poste de travail.

Un utilisateur peut créer un répertoire contenant des données privées en le mentionnant comme tel (confère paragraphe 2.1.1). N'ayant aucun caractère professionnel, les documents contenus dans ce répertoire ne doivent pas être stockés sur le réseau, mais sur le poste de travail.

La personnalisation du poste de travail (fond d'écran, écran de veille, etc.) est tolérée mais ne doit pas porter atteinte à l'image du SIAAP, ni aux obligations de neutralité et de réserve qui s'imposent. Chaque utilisateur doit d'ailleurs faire preuve de décence dans le choix des images ou thèmes utilisés et veiller au respect de la dignité due à l'égard de sa hiérarchie et de ses collègues.

Les utilisateurs doivent verrouiller leur poste de travail dès qu'ils s'absentent un moment, se déconnecter de leur espace personnalisé dès la fin de l'utilisation d'un logiciel ou d'une application, et éteindre leur poste informatique en fin de journée de travail.

Aucune installation d'outils non validés par le SIAAP ne doit être réalisée sur les matériels.

2.1.5. Utilisation de la messagerie

L'utilisation de la messagerie électronique étant destinée principalement aux activités professionnelles, les messages sont soumis aux règles de circulation des écrits professionnels.

Dans le cas d'utilisation de la messagerie pour un usage à titre personnel, les messages reçus ou envoyés doivent comporter une indication suffisamment visible indiquant le caractère privatif, comme cela est explicité dans le paragraphe 2.1.1. L'utilisateur doit supprimer, dans le corps, toute mention relative au SIAAP ou toute autre indication qui pourrait laisser croire que le message est rédigé par l'utilisateur dans le cadre de l'exercice de ses fonctions.

Tout utilisateur peut librement disposer d'un dossier personnel, en le mentionnant comme tel, dans lequel il pourra introduire des fichiers protégés par le secret des correspondances. Toutefois, la sauvegarde et la restauration de cet espace personnel est sous la seule responsabilité de l'utilisateur et la dénomination de cet espace doit faire apparaître, sans ambiguïté, ce caractère privé.

L'utilisateur ne doit pas répondre à des messages non sollicités et ne doit ni envoyer, ni faire suivre un message non sollicité tels que les pourriels, les « hoax », les « chaînes de lettres » ou « chaînes de solidarité ».

La messagerie ne doit en aucun cas être utilisée pour diffuser des propos ou contenus illicites, diffamatoires, injurieux, portant atteinte aux droits ou à la réputation du SIAAP. En aucun cas, la messagerie ne peut servir à stocker des fichiers ou données illicites, à les soustraire à un contrôle de façon générale et/ou à contourner les règles en vigueur.

Les utilisateurs ne doivent pas modifier un message émanant d'un agent ou d'un tiers avant de le faire suivre, de le transférer ou de le communiquer par tout autre moyen, sauf à préciser qu'il s'agit d'un extrait du message d'origine.

En tout état de cause, l'utilisateur doit apprécier si le contenu du message qu'il diffuse n'engage pas la responsabilité de son service ou de sa direction. Si c'est le cas, cette diffusion ne peut se faire qu'en accord avec le supérieur hiérarchique.

La diffusion de message à un grand nombre de destinataires n'est pas autorisée, sauf pour les besoins définis et réglementés, par des personnes habilitées.

L'utilisateur ne doit pas :

- ouvrir des messages dont l'origine, l'objet ou le contenu est douteux, ou exécuter les pièces jointes suspectes. En cas de questions ou de besoin d'ouverture d'un tel message, l'utilisateur avertit l'assistance informatique (adresse de contact : assistance.informatique.telephonique@siaap.fr) ;
- mettre en œuvre une redirection automatique ou une réplication de messages vers une adresse électronique externe ;
- échanger des informations à caractère confidentiel si ce n'est pas indispensable à l'exercice de ses missions.

En cas d'absence prévue, l'utilisateur devra activer le gestionnaire d'absence de la messagerie.

2.1.6. Utilisation de la téléphonie

La téléphonie regroupe les téléphones fixes, sans fil (DECT (Digital Enhanced Cordless Telephone), PMR (Private Mobile Radio), portables GSM (Global System for Mobile Communications)...), accordés selon le profil de poste de l'utilisateur.

L'utilisateur est informé de la traçabilité des communications téléphoniques sur deux aspects :

- enregistrement des numéros des appels émis et reçus (les quatre derniers chiffres sont masqués),
- enregistrement de la durée des communications.

Cela permet de réaliser la taxation téléphonique, afin de mesurer le coût des appels émis.

L'accès au réseau international peut être accordé sur demande, après accord de son directeur, effectuée auprès de l'assistance informatique (contact : assistance.informatique.telephonique@siaap.fr).

L'appel des numéros spéciaux, sans rapport avec les missions professionnelles, est interdit. Dans le cas d'un besoin avéré, une demande peut être effectuée, après accord de son directeur, auprès de l'assistance informatique.

De la même manière que pour la messagerie, si l'utilisateur envoie ou reçoit des SMS personnels, dans une mesure raisonnable, ceux-ci doivent être clairement identifiés par une indication en tête du message (mesure détaillée dans le paragraphe 2.1.2.).

Les SMS non identifiés comme "personnels" émis et reçus sur du matériel appartenant au SIAAP sont susceptibles de faire l'objet de consultation pour des motifs professionnels légitimes.

En cas de perte ou de vol d'un téléphone sans fil ou portable, la procédure implique de prévenir l'assistance informatique en lui adressant une déclaration de perte, signée par son directeur et transmise par mail.

Il est obligatoire de mettre en place un code de verrouillage sur un téléphone portable ou smartphone, afin d'empêcher l'accès d'un tiers aux données présentes en cas de perte.

L'utilisation des smartphones doit se faire en cohérence avec les conditions prévues au forfait.

2.1.7. Utilisation de l'accès à Internet

Les postes de l'informatique industrielle n'ont pas accès à Internet.

Afin d'interdire l'accès à certains sites sans utilité professionnelle ou non autorisés en raison de leur caractère illégal ou immoral (pédophilie, incitation à la haine raciale, apologie de crimes contre l'humanité, révisionnisme, atteintes à la Sécurité Nationale, apologie du terrorisme, trafic de stupéfiants, homophobie, sexisme, pornographie, etc.), un filtrage a été mis en œuvre.

Chaque utilisateur est seul responsable de la décision d'accéder à un site Internet. Le fait que l'accès à un site en particulier ne soit pas interdit ne signifie pas que l'accès à ce site est autorisé et conforme à la réglementation applicable.

Le SIAAP ne pourra être tenu responsable du contenu des sites visités par l'utilisateur, ni des éventuelles compromissions ou mises en cause qui pourraient avoir lieu suite à la visite de ces sites.

Les utilisateurs sont expressément informés que, lorsqu'ils naviguent sur Internet, leur identifiant ainsi que les sites visités sont enregistrés dans les limites prévues par la loi (un an pour les journaux d'activité). Le SIAAP peut effectuer toute opération de contrôle permettant de vérifier le respect des dispositions de la charte ainsi que de la législation applicable. Le SIAAP dispose de statistiques d'utilisation et de traces relatives à ces accès.

Si certains sites non accessibles s'avèrent présenter un intérêt professionnel, il convient d'avertir son supérieur hiérarchique puis l'assistance informatique (contact : assistance.informatique.telephonique@siaap.fr) en fournissant tous les éléments d'étude nécessaires.

2.1.8. Utilisation des services d'accès à distance

Des services d'accès à distance à la messagerie ou à d'autres ressources des Systèmes d'Information sont mis en place.

Les utilisateurs doivent respecter les règles d'utilisation à distance édictées par le SIAAP.

Les utilisateurs peuvent connecter les matériels du SIAAP à des réseaux Wifi (à leur domicile ou lors de déplacements professionnels). Néanmoins, l'utilisateur devra être vigilant afin d'éviter l'introduction de malware (virus, ver, etc.) dans les ordinateurs portables, dans la mesure où la connexion utilisée peut ne pas disposer des protections suffisantes.

Dans les cas d'utilisation des services d'accès à distance, afin de limiter le risque de divulgation d'information, des précautions particulières s'imposent pour protéger contre le vol les équipements mobiles et accessoires utilisés.

2.1.9. Utilisation de matériels personnels

L'utilisation de matériels personnels est interdite sauf pour accéder à distance à la messagerie (Webmail) ou à l'extranet.

2.1.10. Utilisation des réseaux sociaux et sites participatifs

L'accès aux réseaux sociaux est restreint et leur utilisation est susceptible d'être contrôlée par le SIAAP.

Les utilisateurs doivent avoir un usage professionnel de ces ressources. L'utilisation des réseaux sociaux et espaces privatifs à des fins personnelles doit être tout à fait occasionnelle tant en fréquence qu'en durée.

L'attention des utilisateurs est particulièrement attirée sur le respect de règles de confidentialité sur les réseaux sociaux. Il est ainsi rappelé que chaque utilisateur est seul responsable des propos qu'il tient sur les réseaux sociaux et plus largement sur Internet. La responsabilité de chaque utilisateur peut être engagée du fait de ces propos. En particulier, il est demandé à l'ensemble des utilisateurs une attention particulière concernant les informations liées à l'exercice de leur profession qui pourraient être partagées en ligne. En effet, ces informations peuvent toucher à des informations confidentielles (données spécifiques au SIAAP, informations sur des tiers, secret médical, etc.), affecter d'autres individus qui n'ont pas consentis à leur diffusion et/ou projeter une image inexacte et incomplète de certains événements. Le SIAAP appelle donc à la vigilance.

Les utilisateurs ne doivent pas s'exprimer au nom du SIAAP sans y avoir été dûment autorisés.

Les utilisateurs ont un devoir de loyauté et de réserve, tant dans un usage professionnel que personnel des réseaux sociaux.

Les publications, quelle qu'en soit la nature, après validation de la hiérarchie, ne doivent pas porter préjudice au SIAAP, à ses agents ou à tout autre partenaire.

Dans un contexte d'usage personnel, les utilisateurs ne doivent pas utiliser des identifiants et/ou adresses électroniques professionnels.

Les utilisateurs habilités à communiquer à des fins professionnelles sur ces médias, doivent disposer d'un profil professionnel distinct de leur éventuel profil personnel.

Les utilisateurs doivent s'assurer que les informations diffusées sur ces réseaux et sites ne peuvent pas être ré-exploitées à des fins de malveillance informatique ou d'acquisition déloyale d'information.

2.1.11. Traitement des données du SIAAP

Le SIAAP est propriétaire des informations produites par les utilisateurs dans le cadre de leur activité professionnelle et dépositaire des informations confiées.

Les utilisateurs ont le devoir de préserver l'intégrité et la confidentialité des informations qu'ils traitent que ce soit en interne comme à l'extérieur du SIAAP. D'une manière générale, les règles de confidentialité en vigueur pour la communication papier s'appliquent aux supports électroniques et informatiques. Lors de conversations ou de communications téléphoniques dans des lieux publics, le respect des règles de discrétion est particulièrement requis.

Toute communication d'informations confidentielles en dehors du SIAAP doit se faire selon les règles en vigueur et dans le cadre des délégations allouées.

Tout stockage de données du SIAAP sur une plateforme extérieure non validée par le service informatique est interdit (sauf extranet mis en place avec des partenaires dans le cadre de projets)

Les moyens nomades de stockage de masse fournis par le SIAAP (clefs USB, disque dur externe, smartphone, etc.) sont autorisés, mais le SIAAP attire l'attention de l'utilisateur sur une vigilance particulière relative à la sécurité des données présentes sur ces supports (perte, vol, emprunt) et sur les risques associés (virus, etc.).

En informatique industrielle, l'utilisation des ports USB est interdite pour les non-administrateurs.

2.1.12. Traitement des données à caractère personnel

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés précise strictement les conditions légales de la collecte, de l'enregistrement et de la conservation des données à caractère personnel, ainsi que les conditions de leur traitement automatisé.

Le SIAAP est considéré comme responsable des traitements qu'il met en œuvre sur des données à caractère personnel. Un Correspondant Informatique et Libertés (CIL) a été désigné par la Direction Générale du SIAAP. Il est joignable à l'adresse email suivante : correspondant-informatique-liberte@siaap.fr.

Les utilisateurs des Systèmes d'Information s'engagent à respecter, dans le cadre de leur exercice professionnel, les règles issues de la loi « informatique et libertés » susvisée, notamment en ce qui concerne les obligations du responsable de traitement (information des personnes, confidentialité et sécurité des données) et les droits des personnes visées par les traitements (opposition, accès et rectification).

Les utilisateurs ne doivent pas saisir, collecter ou utiliser des données personnelles sensibles, selon les termes de l'article 8 de la loi Informatique et Libertés (religion, opinion politique, santé, vie sexuelle, etc.), des mentions subjectives ou des jugements de valeur pouvant porter atteinte à la dignité ou à la vie privée des personnes, dans les différentes zones de saisies disponibles dans les applications du poste de travail.

Les articles 45 et suivants de la loi « informatique et libertés » prévoient la possibilité pour la Commission Nationale de l'Informatique et des Libertés (CNIL) de prendre des sanctions à l'encontre des personnes qui ne respectent pas les obligations posées par ce texte législatif en matière de traitement de données à caractère personnel.

Conformément aux articles 38 à 43 de la loi « Informatique et Libertés », chaque utilisateur bénéficie de droits spécifiques sur les traitements de données à caractère personnel dont il fait l'objet :

- le droit de regard sur ses propres données personnelles. Il vise aussi bien la collecte des informations que leur utilisation ;
- la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier ;
- le droit d'interroger le responsable d'un fichier ou d'un traitement pour savoir s'il détient des informations sur lui, et le cas échéant d'en obtenir communication ;
- le droit de rectification ou de suppression sur les données le concernant.

Tout utilisateur pourra exercer l'un ou l'autre de ces droits en s'adressant directement au CIL.

2.2. Mesures de précaution

L'utilisateur est responsable de l'usage des ressources auxquelles il a accès.

Afin de contribuer à la sécurité des Systèmes d'Information du SIAAP, l'utilisateur doit adopter un comportement exemplaire qui se traduit notamment par :

- un usage précautionneux des matériels mis à sa disposition ;
- le respect de la configuration matérielle et logicielle initiale des équipements qui sont mis à sa disposition ;
- le rangement sous clé des supports informatiques (CD-Rom, clé USB, etc.) contenant des données confidentielles ;
- la récupération immédiate des documents sensibles qu'il envoie, imprime ou photocopie sur les fax, les imprimantes ou les photocopieurs et l'utilisation systématique de la fonction impression sécurisée ;
- une vigilance importante lors de la récupération de données extérieures au Système d'Information du SIAAP.

Il est conseillé de se reporter au guide des bonnes pratiques mis à la disposition des agents sur l'Intranet.

2.3. Actes illicites

Le Code pénal interdit à tout utilisateur de stocker ou de diffuser tout document proscrit par la loi. Sont concernés notamment par cette interdiction les images et textes :

- pédophiles, pornographiques ;
- homophobes, sexistes ;
- incitant à la haine raciale
- révisionnistes, faisant l'apologie de crimes contre l'humanité ;
- liés aux atteintes à la Sécurité Nationale (apologie du terrorisme, trafic de stupéfiants, etc.) ;
- portant atteinte aux personnes ;
- etc.

Dans le cas où un agent prendrait connaissance ou recevrait à son insu de tels documents, il doit en informer l'Autorité de Police et son supérieur hiérarchique.

Les mêmes sanctions pénales que celles prévues pour les cas listés précédemment sont applicables aux utilisateurs qui accèdent à ces sites Web et participent à des forums traitant de ces sujets.

Les utilisateurs doivent en outre être conscients que ces mêmes sites sont susceptibles de récupérer leurs adresses e-mails et de les utiliser.

En cas de procédure judiciaire pour une infraction présumée aux dispositions énoncées ci-dessus, le SIAAP pourrait être tenu de communiquer à l'autorité judiciaire l'ensemble des éléments d'information qui lui seraient demandés.

3. CONTROLES ET TRAÇABILITE

Les Systèmes d'Information s'appuient sur des fichiers journaux ("logs"), créés en grande partie automatiquement par les équipements informatiques. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement des Systèmes, en protégeant la sécurité des informations du SIAAP, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs accédant aux Systèmes d'Information.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité des Systèmes d'Information.

La mise en œuvre de tout moyen de contrôle et de traçabilité de l'activité des agents doit faire l'objet d'une information préalable auprès des instances représentatives du personnel conformément aux lois et règlementations en vigueur.

Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et les suppressions de fichiers,
- aux connexions entrantes et sortantes au réseau interne, à la téléphonie, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites Web ou le téléchargement de fichiers
- aux badgeages pour mesurer le temps de présence ;
- aux contrôles d'accès pour vérifier les habilitations des accès aux espaces et bâtiments du SIAAP ;
- à la vidéoprotection pour assurer la sécurité des espaces et des personnes ;
- à la taxation téléphonique.

Les agents en charge de ces contrôles sont tenus de respecter la confidentialité des informations auxquelles ils accèdent.

4. SANCTIONS

Le non-respect des règles et obligations édictées dans la charte constituera une faute, susceptible de sanctions disciplinaires et / ou de mesures conservatoires, dans le cadre des règles statutaires.

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des rappels aux règles, des limitations ou suspensions d'utiliser tout ou partie des Systèmes d'Information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

La mise en œuvre et l'utilisation du Système d'Information sont soumises à un ensemble de textes législatifs et réglementaires. Dans le cadre de l'exercice de ses fonctions au quotidien, chaque utilisateur peut être tenu pour responsable civilement ou pénalement en cas de manquement à ces obligations légales et réglementaires.

Une liste non exhaustive des lois et règlements concernés est proposée à l'article « 5. Législation ».

5. LÉGISLATION

La présente charte est établie en considération de la réglementation.

En conséquence, il est rappelé que les utilisateurs doivent notamment respecter, sans que cette liste ait un caractère exhaustif, les réglementations précisées ci-dessous, en vigueur ce jour à et à venir, sachant que leur non-respect peut être sanctionné pénalement :

- Le Code de la Propriété Intellectuelle, qu'il s'agisse de créations multimédia, de logiciels, de textes, de photos, d'images, de toute nature, étant souligné que toute mention relative aux droits d'auteur ne peut faire l'objet d'une suppression et que toute reproduction, adaptation ou modification de l'œuvre de celui-ci sans son consentement constitue une contrefaçon,
- Le Code Pénal et notamment les dispositions issues de la loi Godfrain n° 88-19 du 5 janvier 1988 relative à la fraude informatique,
- La loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,
- La loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet, dite loi Hadopi ou loi création et Internet,
- La loi n°2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet,
- La loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés,
- La loi n°83634 du 13 juillet 1983 portant droits et obligations des fonctionnaires,
- La loi n°2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels.

6. DÉFINITIONS

- **Administrateur technique :** personne qui a pour rôle d'assurer le bon fonctionnement des Systèmes d'Information de l'entreprise ou d'une partie d'un système, d'un logiciel, etc. Pour mener à bien sa mission, il dispose de pouvoirs et de droits d'accès étendus sur les Systèmes d'Information.
- **Confidentialité :** fait d'assurer que l'information n'est accessible qu'aux personnes autorisées. La confidentialité est une obligation légale pour les données personnelles.
- **Correspondant Informatique et Libertés (CIL) :** agent d'une entreprise ou d'un organisme public dont la fonction est de veiller au respect de la réglementation en matière de données privées au sein de sa structure, plus particulièrement à la bonne application de la loi Informatique et Libertés. Il doit créer, mettre à jour et publier un registre public dans lequel il inscrit l'ensemble des traitements effectués (il s'agit des opérations concernant les informations nominatives). Il assure également une fonction de conseil, de recommandation et d'alerte auprès des responsables des traitements. Enfin, il exerce une mission d'intermédiaire entre son organisme et la Commission Nationale de l'Informatique et des Libertés (CNIL).
- **Donnée personnelle :** toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.
- **Droit à la déconnexion :** droit pour un salarié de ne pas être connecté à ses outils numériques professionnels en dehors de son temps de travail.
- **Droits d'accès :** périmètre de ce à quoi il est possible d'accéder avec un identifiant et un mot de passe. Ils sont différents d'un utilisateur à l'autre en fonction de ses missions.
- **Intégrité :** fait que des données ayant été envoyées, reçues ou stockées sont exactes, complètes et n'ont pas été modifiées de façon fortuite, illicite ou malveillante.
- **Politique de sécurité des Systèmes d'Information (PSSI) :** document établi au sein d'une entreprise ou d'une collectivité afin de définir un certain niveau de sécurité. La PSSI reflète la vision stratégique de la direction en matière de Sécurité des Systèmes d'Information.
- **Réseau :** moyens mis en place par le SIAAP pour relier les composants matériels (ordinateurs, imprimantes, serveurs…) et les utilisateurs entre eux et aux Systèmes d'Information, et éventuellement à Internet.
- **Ressources :** désigne l'ensemble des composants matériels (ordinateurs, imprimantes, serveurs…) et immatériels (connaissances, savoir-faire, applications, base de données, procédures…) détenus par les le SIAAP et ses collaborateurs, contribuant à la collecte, à la création et au traitement de l'information, et à l'atteinte des objectifs du SIAAP.
- **Référent Sécurité des Systèmes d'Information (RSSI) :** personne chargée de la définition et de la mise en œuvre de la politique de sécurité des Systèmes d'Information, qui consiste à garantir la disponibilité, la sécurité, et l'intégrité des Systèmes d'Information et des données.
- **Service d'accès à distance de la messagerie :** service fourni aux agents ayant une boîte mail, permettant l'accès à la messagerie Internet du SIAAP depuis un poste de travail situé en dehors des locaux du SIAAP en utilisant une connexion Internet. Cet accès se fait par l'intermédiaire de https://webmail.siaap.fr.
- **Systèmes d'Information :** ensemble composé de ressources (matériels, logiciels, données et procédures), permettant de collecter, regrouper, classifier, traiter et diffuser de l'information sur un environnement donné.
- **Traitement de données à caractère personnel :** toute opération ou tout ensemble d'opérations portant sur des données à caractère personnel et notamment, la collecte, l'enregistrement, la transmission, la communication, l'effacement ou la destruction.
- **Utilisateur :** tout agent du SIAAP, stagiaire, prestataire ou toute personne à laquelle un quelconque droit d'accès à tout ou partie des Systèmes d'Information du SIAAP est accordé.

SIAAP

Service public de l'assainissement francilien

La charte informatique en 10 points

Travailler ensemble sur un même système d'information implique des règles communes.

La charte, disponible sur l'Intranet, définit les principaux droits et devoirs des utilisateurs des ressources informatiques et de communication.

Tous les agents et les partenaires du SIAAP s'engagent à l'appliquer.

1. **Mot de passe** : il est personnel, confidentiel, incessible.

2. **Traitement des données à caractère personnel** : la création et la tenue de fichiers contenant des données personnelles sont soumises à déclaration et accord préalable du Correspondant Informatique et Liberté.

3. **Utilisation des données du SIAAP** : afin de préserver leur intégrité et leur confidentialité, le transfert et le stockage des données du SIAAP sur une plateforme extérieure non validée par le SIAAP ne sont pas autorisés.

4. **Usage personnel des fichiers et des correspondances (dossiers, mails, SMS)** : l'utilisateur doit indiquer une mention « personnel » ou « privé », sinon l'information concernée est considérée comme professionnelle et peut être consultée par le SIAAP en l'absence de la personne.

5. **Droit à la déconnexion** : droit d'un agent de ne pas être connecté à ses outils numériques professionnels en dehors de son temps de travail.

6. **Déconnexion informatique** : tout utilisateur doit se déconnecter systématiquement du système ou d'un logiciel, ou verrouiller sa session dès la fin de l'utilisation.

7. **Traçabilité de l'activité des utilisateurs** : plusieurs applications du SIAAP permettent d'assurer une traçabilité de l'activité des utilisateurs dans le cadre professionnel, par exemple pour assurer la sécurité des personnes et des accès (vidéoprotection), permettre la taxation téléphonique, connaître les sites Internet visités, etc.

8. **Filtrage des accès à Internet** : cette mesure est mise en place afin d'interdire l'accès à certains sites illégaux ou sans utilité professionnelle.

9. **Prévention contre les logiciels malveillants:** les utilisateurs ne doivent pas ouvrir de mails suspects, installer de logiciel sur leur poste, utiliser de clés USB non vérifiées, etc.

10. **Réseaux sociaux** : leur utilisation implique le respect des règles de confidentialité, du devoir de loyauté et de réserve vis-à-vis du SIAAP.