Accusé de réception en préfecture
044-200014926-20190926-2019-37a-DE
Date de télétransmission : 17/10/2019
Date de réception préfecture : 17/10/2019

CHARTE INFORMATIQUE

INTRODUCTION

Le SYDELA met en œuvre un système d'information et de communication nécessaire à l'exercice de ses missions. Il met ainsi à disposition de ses collaborateurs des outils informatiques et de communication.
La présente charte définit les conditions d'accès et d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication du SYDELA.
Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées, que l'utilisation ait lieu dans ou en dehors des locaux du SYDELA. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et / ou pénale ainsi que celle du SYDELA.

I. LE CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à tout utilisateur du Système d'Information et de communication du SYDELA pour l'exercice de ses activités professionnelles. L'utilisation à titre privé de ces outils est tolérée, mais doit être raisonnable et ne pas perturber le bon fonctionnement du service.
Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques recommandées.

Quelques définitions :
On désignera sous le terme « **utilisateur »** toute personne autorisée à accéder aux outils informatiques et aux moyens de communication du SYDELA et à les utiliser : agents, élus, personnels de sociétés prestataires, visiteurs occasionnels, etc.
Les termes "**outils informatiques et de communication**" recouvrent tous les équipements informatiques, de télécommunications et de reprographie du SYDELA.
Le **responsable de traitement** est la personne qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. Pour tous ceux mis en œuvre dans le cadre des activités du SYDELA, c'est ce dernier qui en est le responsable, représenté par son Président.

II. LES RÈGLES D'UTILISATION DES SYSTÈMES D'INFORMATION DU SYDELA

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par le SYDELA. L'accès aux Systèmes d'information du SYDELA (poste de travail, applications, messagerie, Internet, téléphone…) est fourni à l'utilisateur pour l'exercice de son activité professionnelle.

1. Le rôle du service organisation et systèmes d'information

Le service organisation et systèmes d'information met en place et assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication du SYDELA. Les agents habilités de ce service disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.
Les prestations techniques peuvent être sous-traitées et les intervenants peuvent avoir les mêmes droits, en fonction des missions qui leur sont confiés, ainsi que les mêmes obligations.
Ils ont accès à l'ensemble des données techniques et s'engagent à respecter les règles de confidentialité applicables aux contenus des documents.

Ils sont assujettis au devoir de réserve, au secret et à la discrétion professionnelle et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.
En cas de non-respect des règles énoncées dans cette charte, les agents habilités du service Organisation et Systèmes d'Information ou le DPD les rappellent à l'intéressé. En cas de récidive, ils peuvent saisir sa hiérarchie après information du Directeur Général des Services. Ils ne peuvent être contraints à agir dans un sens contraire aux dispositions énoncées dans cette charte.

2. Le rôle du délégué à la protection des données

Le règlement européen sur la protection des données personnelles (RGPD) et la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés définissent les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elles ouvrent aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte.
Le SYDELA a désigné un délégué à la protection des données à caractère personnel. Ce dernier a pour mission de veiller au respect des dispositions du Règlement européen sur les données personnelles et des lois nationales.
Le délégué à la protection des données est principalement chargé :

- d'informer et de conseiller le responsable de traitement ou les sous-traitants,
- de contrôler le respect du règlement et du droit national en matière de protection des données, notamment de veiller aux droits des personnes ;
- de conseiller le SYDELA sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Il est obligatoirement consulté par le responsable des traitements préalablement à leur création.
Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel du SYDELA au fur et à mesure de leur mise en œuvre.
Il a accès à l'ensemble des documents et données de façon à exercer sa fonction de contrôle.

3. Responsabilité de l'utilisateur

L'utilisateur est responsable de l'usage qu'il fait des outils et matériels informatiques sous le contrôle du service organisation et systèmes d'information.
L'utilisateur peut consulter certains de ses outils à distance (messagerie, logiciels, espaces réseaux). L'utilisateur veille à avoir un usage modéré et contrôlé des outils informatiques pendant et en-dehors du temps de travail, notamment de la messagerie, afin d'éviter une éventuelle surinformation, une baisse de la productivité et une baisse de la concentration.
L'utilisateur doit en outre respecter les législations et réglementations en vigueur, particulièrement en ce qui concerne :

- Les droits des usagers,
- La propriété littéraire, intellectuelle et artistique : interdiction de réaliser ou d'utiliser des copies illicites d'éléments (logiciels, images, textes, musiques…) protégés par la loi de la propriété intellectuelle,
- La protection des données personnelles et sensibles,
- La gestion, le versement, la destruction des archives publiques, courriels, documents et données. Le tri et l'archivage régulier permettent une bonne gestion de l'information.

L'utilisateur doit protéger les informations placées sous sa responsabilité et en particulier :

- Respecter les mesures de sécurité associées au niveau de confidentialité des informations qu'il traite,
- Respecter la confidentialité des informations lors de toutes les phases de leur cycle de vie : création, stockage, transmission, impression, suppression…

L'utilisateur s'engage à sauvegarder régulièrement ses documents professionnels sur des espaces réseaux partagés selon un plan de classement (arborescence) défini par le SYDELA , et notamment pas en local sur son disque dur (C :), ce dernier n'étant pas sauvegardé. Il identifie également les messages professionnels les plus importants : messages stratégiques, à valeur juridique forte, engageants, messages dont la perte peut générer des risques pour le SYDELA, messages liés à un dossier en cours, messages permettant de comprendre le suivi d'un dossier ou portant une décision sur une affaire.
L'utilisateur est conscient d'accéder à des données à caractère personnel, sensible ou confidentiel et s'engage donc à ce titre, au respect du secret professionnel et à la discrétion, conformément à ses obligations statutaires et à sa déontologie.
En ce qui concerne les données personnelles ou sensibles, l'utilisateur s'engage ainsi à :

- respecter les règles mises en place par le délégué à la protection des données ;
- 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 à ce que cela soit nécessaire 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 ses données;
- en cas de cessation de ses fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Tous les soirs, l'utilisateur doit ranger son matériel informatique dans des placards ou tiroirs de telle sorte qu'ils ne soient pas visibles depuis l'extérieur.

L'utilisateur a également une démarche de développement durable avec les outils mis à sa disposition, notamment en éteignant les postes de travail et les écrans à chaque absence (sauf demande expresse du service organisation et systèmes d'information).
L'utilisateur est également responsable de la bonne application de la charte par les personnels de société prestataires, visiteurs, élus qui seraient amenés à utiliser les moyens informatiques du SYDELA sous sa responsabilité.

4. L'authentification

Le SYDELA peut mettre à la disposition de l'utilisateur différents moyens d'authentification, dont le choix est déterminé par le service organisation et systèmes d'information : identifiants, mots de passe plus ou moins complexes, badges, clés, etc. L'accès aux ressources informatiques peut être limité en fonction des besoins réels et des contraintes imposées par le partage de ces ressources avec d'autres utilisateurs. Les accès cessent avec la disparition des raisons qui ont motivé leur attribution ou par décision motivée de l'autorité territoriale, notamment si le comportement d'un utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.
L'accès aux ressources informatiques repose sur l'utilisation d'un compte (nom d'utilisateur et mot de passe) fourni à l'utilisateur lors de son arrivée. Lors de la première connexion aux ressources informatiques du SYDELA, l'utilisateur a pour obligation de changer son mot de passe, qui est alors connu de lui seul.

Les moyens d'authentification sont personnels et confidentiels.

L'agent est tenu d'organiser toute absence programmée et ainsi :

- s'organiser et mettre à la disposition de son service tous les documents ou outils nécessaires. Le mot de passe de l'agent ne doit pas être communiqué ;
- informer ses interlocuteurs grâce au gestionnaire d'absence du bureau de la messagerie et indiquer le contact vers lequel les messages devront être relayés.

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler au service organisation et systèmes d'information toute violation ou tentative de violation suspectée de son compte réseau
- Ne jamais confier son identifiant/mot de passe.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramétrages de sécurité du poste de travail.
- Ne pas installer de logiciels sans licence. Et lors de l'installation veiller à ne pas installer des applications supplémentaires ou des logiciels susceptibles de porter à atteinte à la sécurité informatique du SYDELA.
- Ne pas copier, modifier, détruire les logiciels propriétés du SYDELA.
- Appliquer une règle de mise en veille de sa session suivant les préconisations du service Organisation et Systèmes d'Information.
- Verrouiller ou éteindre son ordinateur dès qu'il quitte son poste de travail, même momentanément.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Toute copie de données sur un support externe ou transmission à un interlocuteur par quelque moyen que ce soit est autorisée sous réserve du respect des préconisations de cette charte informatique. Cette autorisation ne concerne pas les données personnelles et sensibles.

En outre, il convient de rappeler que les visiteurs peuvent avoir accès aux Systèmes d'Information du SYDELA sous la responsabilité des utilisateurs qui les y autorisent.
Les contrats signés entre le SYDELA et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant leurs obligations.

III. LES MOYENS INFORMATIQUES

1. Configuration du poste de travail

Le SYDELA met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions. Seuls les équipements validés et répertoriés par le service organisation et systèmes d'information du SYDELA sont autorisés.

L'utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle.
- Modifier des éléments de configuration au-delà des limites portant atteinte aux performances du poste de travail tels que veilles animées, curseurs animés, etc.
- Connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par le service organisation et systèmes d'information.
- Nuire au fonctionnement des outils informatiques et de communications.

- Personnaliser son poste de travail avec des éléments dont le contenu est contraire à la loi, l'ordre public ou aux bonnes mœurs, et met en cause l'intérêt et la réputation de l'institution.

Toute installation de logiciels supplémentaires est subordonnée à l'accord du service organisation et systèmes d'information.

Il doit signaler tout dysfonctionnement ou fonctionnement anormal du matériel informatique au service Organisation et Systèmes d'information

2. Equipements nomades

On entend par « **équipements nomades** » tous les moyens techniques mobiles (ordinateur portable, téléphones mobiles ou smartphones, CD ROM, clé USB, disque dur externe, etc.).
Quand un ordinateur portable ou un autre équipement nomade se trouve dans le bureau de l'utilisateur qui en a l'usage ou dans un espace partagé, cet ordinateur doit être rangé à l'abri des regards et, dans la mesure du possible, dans du mobilier sécurisé.
Afin de garantir la sécurité des données, les ordinateurs portables qui sortent des locaux du SYDELA peuvent être cryptés, suivant les préconisations du service Organisation et Systèmes d'Information Néanmoins, l'utilisateur ne doit emmener sur son équipement mobile que les données qui lui sont strictement nécessaires à l'accomplissement de ses missions pendant le temps de son déplacement. Il ne doit pas copier de données à caractère personnel (au sens du Règlement Général de Protection des Données (RGPD)) sur son équipement mobile sauf accord explicite par le délégué à la protection des données.
L'utilisation de smartphones pour relever la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté (code PIN notamment) de manière à prévenir tout accès non autorisé aux données qu'ils contiennent. Le service Organisation et Systèmes d'Information pourra mettre en œuvre des outils de gestion rendant ces protections techniquement obligatoires.
Il est nécessaire de faire preuve d'une vigilance particulière dans les lieux publics en ne laissant pas les équipements sans surveillance, notamment lorsque l'accès n'est pas contrôlé.
L'utilisateur doit signaler au service organisation et systèmes d'information, le plus rapidement possible, toute perte ou vol d'un équipement.
En cas de possession d'un ordinateur portable, il est nécessaire de se connecter régulièrement au réseau informatique du SYDELA pour s'assurer de la bonne mise à jour du logiciel anti-virus et de l'application des correctifs de sécurité.
Par ailleurs, des équipements mobiles (téléphones, tablettes, …) peuvent être mis à disposition de certains utilisateurs pour répondre à des besoins professionnels identifiés et validés par l'autorité territoriale. Dans certains cas, ces équipements peuvent permettre d'utiliser des applications gratuites, téléchargeables directement, indépendamment des usages professionnels. Ces usages privés sont admis dans la mesure où l'utilisateur en assume l'entière responsabilité, aussi bien en termes d'usage, de droit d'usage que de maintenance, et qu'ils ne nuisent pas au bon fonctionnement des applications nécessaires au SYDELA pour l'accomplissement de ses missions.

En cas de dysfonctionnement, le service organisation et systèmes d'information apportera un service de maintenance limité aux applications professionnelles et ne sera en aucun cas responsable des interactions éventuelles avec les applications privées de l'utilisateur.

3. Matériels partagés

L'utilisateur d'un équipement nomade ou d'un matériel spécifique partagé dans le cadre de l'activité professionnelle (vidéoprojecteur, …) en assure la garde et la responsabilité. Il est tenu de déclarer tout incident (perte, vol, dégradation) et de procéder aux démarches telles que la déclaration de vol ou de plainte. 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.

4. Internet et réseaux sociaux

L'utilisateur peut consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle.
Certains usages de l'Internet sont de nature à ralentir les temps d'accès au réseau et peuvent gêner les autres utilisateurs, voire porter atteinte à l'intégrité du système d'information. Ainsi ils doivent être limités et utilisés exclusivement en cas de nécessité de service :

- Télécharger des fichiers,
- Ecouter la radio en ligne,
- Regarder des vidéos, des films, écouter de la musique.

Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, l'ordre public ou aux bonnes mœurs, et ne met pas en cause l'intérêt et la réputation de l'institution, ni la performance du réseau, est admise.
Les devoirs de réserve, de secret et de discrétion professionnels s'appliquent également sur les réseaux sociaux, lorsqu'un agent participe à des conversations sur Internet qui citent ou impliquent le SYDELA, ses élus ou ses agents.
En particulier, l'utilisateur applique les règles suivantes à tous les réseaux sociaux, à toutes les publications et les commentaires qui impliquent directement ou indirectement le SYDELA ou un collègue :

- Ne publier aucun propos qui pourrait nuire à la réputation du SYDELA ou à un collègue.
- Ne divulguer et ne transmettre aucune information ni aucun document.
- Si l'utilisateur revendique son appartenance au SYDELA sur son profil, il ne doit pas y avoir d'ambiguïté sur le fait qu'il ne le représente pas.

Il est rappelé que les obligations des agents s'étendent à la sphère privée et que tout manquement commis même en-dehors du cadre professionnel est susceptible d'être sanctionné.

5. Messagerie électronique

a) Conditions d'utilisation

La messagerie mise à disposition de l'utilisateur est destinée à un usage professionnel.
L'utilisateur est responsable des messages émis avec son adresse de messagerie (avec suffixe @sydela.fr, qui apparaît systématiquement en tête de tous ses messages) : selon le contenu, il peut engager sa collectivité.

Un message électronique peut constituer une preuve et peut engager son expéditeur et avoir un effet juridique sur son destinataire : tout engagement pris par un agent de manière explicite, même de manière irrégulière, est de nature à engager la collectivité.
Tout message reçu à titre professionnel doit être enregistré dans l'arborescence suivant les consignes de son service. Tout message qui ne serait pas traité de cette manière alors qu'il aurait dû l'être engagera la responsabilité de son destinataire.
Les diffusions de type petites annonces, chaînes, message à caractère politique, philosophique, religieux, humanitaire, etc. ne sont pas autorisées (les messages à vocation non professionnelle sont uniquement autorisés sur le panneau d'affichage prévu à cet effet).
Les messages de nature discriminatoire, diffamatoire, pédophile, pornographique ou d'incitation à la violence ou la haine raciale ou constituant des actes de harcèlement ou d'agression ou d'injures sont constitutifs d'infractions pénales et de fautes professionnelles sanctionnables.
L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail de l'agent ni la sécurité du réseau informatique du SYDELA.

Tout message qui s'avèrerait à caractère personnel, notamment par la mention PRIVÉ ou PERSONNEL dans l'objet, bénéficiera du droit au respect de la vie privée et du secret des correspondances. À défaut, il est présumé professionnel et le SYDELA pourra en prendre connaissance pour assurer ses missions. Toutefois, un juge d'instruction ou un officier

de police judiciaire peut procéder à la saisie des données à caractère personnel nécessaires à la manifestation de la vérité, notamment dans le cas d'une procédure judiciaire. En cas de doutes sérieux sur le respect par l'utilisateur de son devoir de confidentialité, de discrétion, ou de respect de ses obligations professionnelles, l'employeur pourra consulter les messages susceptibles de caractériser cette infraction, en présence de ce dernier ou en son absence après l'avoir appelé et si ce dernier ne rappelle pas ou ne peut pas se déplacer dans des délais raisonnables ; ce dernier sera alors considéré comme dûment appelé.
L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par le service organisation et systèmes d'information, et validées par le Directeur Général des Services, en particulier en ce qui concerne :

- La volumétrie de la messagerie,
- La taille maximale de l'envoi et de la réception d'un message,
- La gestion de l'archivage de la messagerie.

Le transfert de messages à caractère professionnel, ainsi que leurs pièces jointes, sur des messageries personnelles n'est pas autorisé.

En cas de réception de message douteux, l'utilisateur ne doit pas l'ouvrir et notamment pas les éventuelles pièces jointes et prévenir sans délai le service Organisation et Systèmes d'Information. En cas de demande d'informations sensibles, l'utilisateur portera une attention particulière à la vérification de l'émetteur du message afin d'éviter toute tentative de fraude ainsi qu'à sa réelle habilitation à recevoir ces informations.

A des fins de sécurité, le service Organisation et Systèmes d'Information pourra préconiser certaines configuration que l'Utilisateur sera tenu de respecter (non affichage automatique des images dans la messagerie par exemple).

b) Accès à la messagerie d'un agent pendant son absence

En cas d'absence d'un agent et afin de ne pas interrompre le fonctionnement du service, le service organisation et systèmes d'information peut ponctuellement accéder à la boîte aux lettres individuelle de l'agent dans le cadre restrictif suivant :

- La demande d'accès est établie par le supérieur hiérarchique de l'agent, qui vérifiera préalablement qu'aucun autre moyen n'a pu être mis en œuvre pour assurer la continuité du service.
- La demande d'accès a obtenu l'accord du Directeur Général des Services.
- Le demandeur identifiera auprès du service organisation et systèmes d'information le message ou les dossiers électroniques à caractère exclusivement professionnel, et identifiés comme tel par son objet et/ou son expéditeur, à lui transférer ou le message d'absence à apposer. Il n'a pas accès aux autres messages de l'agent.
- L'agent concerné est informé dès que possible des messages transférés et contactera le service organisation et systèmes d'information pour obtenir son mot de passe provisoire.

Cette procédure peut impliquer que le service organisation et systèmes d'information accède à la messagerie de l'utilisateur, supprime son mot de passe et lui affecte un mot de passe provisoire qu'il appartiendra à l'utilisateur de modifier à sa première connexion.

Ces dispositions exceptionnelles motivées par le seul intérêt du service peuvent également s'appliquer au départ d'un agent (mutation, mise en disposition, détachement ou décès), au moment de la suppression définitive de son compte bureautique et de la réaffectation de ses équipements.

c) Courriel non sollicité

Le SYDELA dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, l'utilisateur est invité à limiter son consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et

de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

d) Signature

La signature doit être conforme à la charte graphique du SYDELA. A cet effet, l'utilisateur doit utiliser le modèle de signature qui aura été mis à sa disposition au préalable.

6. Espaces de stockage de fichiers

Un espace appelé « Pro-Privé » est mis à disposition de chaque agent sur demande auprès du service organisation et systèmes d'information. Cet espace est accessible uniquement par l'agent et l'administrateur système.
On entend par espace pro-privé un espace qui est utilisé pour stocker des fichiers personnels à vocation professionnelle mais non nécessaires au SYDELA.
Cet espace est supprimé à la demande ou au départ de l'agent.
La copie de fichiers professionnels sur un autre ordinateur que celui fourni par le SYDELA n'est pas autorisé.

Tout dossier ou fichier qui s'avèrerait à caractère personnel, notamment par la mention PRIVÉ ou PERSONNEL dans son nom, bénéficiera du droit au respect de la vie privée. À défaut, il est présumé professionnel et le SYDELA pourra en prendre connaissance pour assurer ses missions. Toutefois, un juge d'instruction ou un officier de police judiciaire peut procéder à la saisie des données à caractère personnel nécessaires à la manifestation de la vérité, notamment dans le cas d'une procédure judiciaire. En cas de doutes sérieux sur le respect par l'utilisateur de son devoir de confidentialité, de discrétion, ou de respect de ses obligations professionnelles, l'employeur pourra consulter les fichiers susceptibles de caractériser cette infraction, en présence de ce dernier ou en son absence après l'avoir appelé et si ce dernier ne rappelle pas ou ne peut pas se déplacer dans des délais raisonnables ; ce dernier sera alors considéré comme dûment appelé.

7. Téléphone

Le SYDELA met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.
L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.
Le SYDELA ne met pas en œuvre un suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Pour les fixes et mobiles, les logiciels de taxation enregistrent dates, heures des appels sortants avec durées, coûts et numéros appelés.
Les données peuvent être stockées afin de permettre le contrôle des factures et les statistiques de consommation. Le service en charge de la téléphonie vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.
Le SYDELA s'interdit d'accéder à l'intégralité des numéros appelés via les téléphones fixes mis en place et via les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, le service en charge de la téléphonie, sur demande du Directeur Général des Services, se réserve le droit d'accéder aux numéros complets des relevés individuels.

8. Modèles de documents

Les documents produits par les utilisateurs doivent être conformes aux modèles fournis par le SYDELA et suivant la charte graphique définie.

9. L'utilisation des outils informatiques par les représentants du personnel

Les représentants du personnel utilisent, dans le cadre de leur mandat, les outils informatiques qui leur sont attribués pour l'exercice de leur activité professionnelle.

IV. L'ADMINISTRATION DES SYSTÈMES D'INFORMATION

Des moyens de supervision et de contrôle sont mis en œuvre afin de garantir un nécessaire équilibre entre le respect des libertés individuelles et les intérêts légitimes de la collectivité exprimés par l'autorité territoriale. Ces moyens impliquant la collecte de données les concernant et conformément au règlement européen sur la protection des données personnelles (RGPD) et à la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, les agents ont, notamment, la possibilité d'accéder aux données les concernant enregistrées par les moyens de supervision inscrits dans le présent article, et de connaître le responsable et les destinataires du traitement. L'utilisateur devra faire sa demande par écrit à l'autorité territoriale du SYDELA en justifiant de son identité. Dans les mêmes conditions, tout utilisateur peut demander au responsable d'un traitement que soient, selon les cas et dans la limite des informations utiles à la collectivité, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel le concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

1. Les systèmes automatiques de filtrage

L'utilisateur est tenu de respecter l'ordre public et les bonnes mœurs : ne pas manipuler des informations contraires aux principes énoncés ci-dessus (accès à des sites Internet, stockage ou diffusion de fichiers, envoi de fichiers...), notamment des informations à caractère injurieux, diffamatoire, raciste, xénophobe, pornographique, pédophile ou pouvant constituer une incitation à la haine, la violence ou de prosélytisme notamment en faveur de sectes.
À titre préventif, des systèmes automatiques de filtrage permettant donc de diminuer les flux d'information pour le SYDELA et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (peer to peer, ...).

2. Les systèmes automatiques de traçabilité

Le service organisation et systèmes d'information du SYDELA opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements des systèmes d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité (détection des spams et des virus notamment).
Il s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information.
Le service organisation et systèmes d'information est le seul utilisateur de ces informations.

a) Les fichiers de journalisation pour Internet :

Ces fichiers comportent les données suivantes :

- Adresse URL des sites consultés,
- Date et heure des connexions,
- Identifiant utilisé pour la connexion,
- Sites les plus consultés,
- Volume des données reçues et transmises.

l'Utilisateur sera informé par le service Organisation et Systèmes d'Information en cas de modification de la liste des informations enregistrées.
En cas d'utilisation manifestement abusive d'Internet sur un poste, une liste détaillée des accès de l'agent peut être adressée ponctuellement au Directeur Général des Services, à sa demande écrite auprès du service organisation et systèmes d'information. Les limites de durée de conservation des données s'imposent à lui de la même façon. L'agent titulaire du poste devra être informé de cette demande par sa hiérarchie.

b) Les fichiers de journalisation pour la messagerie :

Les informations enregistrées pour chaque message électronique entrant ou sortant sont :

- Emetteur du message,

- Destinataire du message,
- Date et heure de traitement du message.

l'Utilisateur sera informé par le service Organisation et Systèmes d'Information en cas de modification de la liste des informations enregistrées.

3. Gestion du poste de travail

À des fins de maintenance informatique, le service organisation et systèmes d'information peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur.
Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le service informatique peut être amené à intervenir sur l'environnement technique des postes de travail (mise à jour de logiciels, …). Il s'interdit d'accéder aux contenus.

V. PROCÉDURE APPLICABLE LORS DU DÉPART DE L'UTILISATEUR

Lors de son départ, l'utilisateur doit restituer aux personnes habilitées du service organisation et systèmes d'information les matériels mis à sa disposition.
Il doit préalablement effacer ses fichiers et données privées, y compris de sa messagerie car son contenu est susceptible d'être archivé. Toute copie de documents professionnels est autorisée sous réserve du respect du secret professionnel, de la discrétion professionnelle et du devoir de réserve.
Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés après son départ.

VI. RESPONSABILITÉS- SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre.
Des sanctions en interne peuvent être prononcées, elles consistent :
• dans un premier temps, en un rappel à l'ordre émanant du Directeur Général Des services, en cas de non-respect des règles énoncées par la charte ;

• dans un second temps, et en cas de renouvellement, après avis du Directeur Général des Services et du supérieur hiérarchique de l'agent, en des sanctions disciplinaires.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information est de plus susceptible de sanctions pénales prévues par la loi.

VII. OPPOSABILITÉ DE LA CHARTE

Toute utilisation ou accès aux systèmes d'information du SYDELA vaut acceptation entière et sans réserve de la présente charte.

VIII. ENTRÉE EN VIGUEUR DE LA CHARTE

La présente charte a été adoptée après information et consultation du comité technique et délibération du comité en date du 26 septembre 2019.
Elle est applicable à compter du 16 octobre 2019.