Accusé de réception en préfecture
067-200067783-20211028-211028D7-DE
Date de télétransmission : 02/11/2021
Date de réception préfecture : 02/11/2021

COMMUNAUTÉ DE COMMUNES
HANAU LA PETITE PIERRE

CHARTE INFORMATIQUE

Version	Date d'entrée en vigueur	Nature / Raison de la modification	Pages concernés
1	01/01/2018	Version initiale	Toutes
2	01/11/2021	Mise à jour n°1	Toutes

Table des matières

Introduction

La Communauté de Communes de Hanau La Petite Pierre (CCHLPP) met en œuvre un système d'information et de communication (S.I.C.) nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des outils mobiles. Les agents, dans l'exercice de leurs fonctions, sont conduits à utiliser les outils informatiques et téléphoniques mis à leur disposition et à accéder aux services de communication de l'établissement public.

L'utilisation du S.I.C. doit se faire exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du S.I.C., la présente charte pose les règles relatives à l'utilisation de ces ressources. Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation mise en place, non seulement pour la bonne exécution du contrat de travail des agents, mais aussi dans le cadre de la responsabilité pénale et civile de l'employeur. Elle dispose d'un aspect réglementaire et est annexée au règlement intérieur de l'établissement public. Elle ne remplace en aucun cas les lois en vigueur que chacun est censé connaître.

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 de l'établissement public.

Protection des données à caractère personnel

Le Règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et communément appelé Règlement Général sur la Protection des Données (RGPD) est entré en vigueur le 25 mai 2018.

Le RGPD, complété par la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa version consolidée du 20 juin 2018, impose les conditions dans lesquelles des traitements de données à caractère personnel peuvent être réalisés. Cette réglementation ouvre aux personnes concernées par les traitements un droit d'information, d'accès, de rectification, d'effacement, de portabilité et d'opposition des données enregistrées sur leur compte.

L'établissement public a désigné un Délégué à la Protection des Données à caractère personnel (DPO). Ce dernier a pour mission de veiller au respect des dispositions du RGPD Il a pour rôle de s'assurer de la conformité juridique des traitements.

Il est obligatoirement consulté par le responsable de traitement préalablement à la création d'un fichier. Le « Responsable de Traitement » est celui qui détermine les finalités et les moyens du traitement, c'est celui qui a pris l'initiative du traitement.

Il recense dans un ou plusieurs registres la liste de l'ensemble des traitements de données à caractère personnel de l'établissement public au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande. Elle est également diffusée sur l'intranet de la CCHLPP

Le correspondant veille au respect des droits des personnes citées ci-dessus. En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le DPO (Vianney WICKERSHEIMER dpo@hanau-lapetitepierre.alsace).

Champ d'application

Quelques définitions

On désignera sous le terme « *Utilisateur* » toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de l'établissement public et à les utiliser : agents permanents, agents occasionnels, élus, prestataires et collaborateurs extérieurs, visiteurs occasionnels.

Les termes « *Outils Informatiques et de Communication* » recouvrent tous les équipements informatiques, de télécommunications et de reprographie de l'établissement public.

Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du S.I.C. de l'établissement public, quel que soit leur statut, y compris les agents permanents, agents occasionnels, élus, prestataires et collaborateurs extérieurs, visiteurs occasionnels.

Les agents veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au S.I.C.

S.I.C.

Le S.I.C. de l'établissement public est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques y compris clés USB, réseau informatique (serveurs, switchs, routeurs et connectique), photocopieurs, télécopieurs, téléphones, smartphones, tablettes et clés 4G, écrans numériques interactifs, logiciels, fichiers, données et bases de données, système de messagerie, connexion internet, intranet, extranet, abonnements à des services interactifs.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du S.I.C. le matériel personnel des agents connecté au réseau de l'établissement public, ou contenant des informations à caractère professionnel concernant l'établissement public.

Autres accords sur l'utilisation du S.I.C.

La présente charte ne préjuge pas des accords particuliers pouvant porter sur l'utilisation du S.I.C. par les institutions représentatives, l'organisation d'élections par voie électronique ou la mise en télétravail de agents.

Règles d'utilisation du S.I.C.

Les modalités d'intervention du service informatique

Le service de l'informatique interne assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de l'établissement public. Le personnel de ce service dispose d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Ils ont accès à l'ensemble des données techniques et respectent les règles de confidentialité applicables aux contenus des documents.

Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à traiter dans le cadre de leurs fonctions.

L'authentification

L'accès à certains éléments du S.I.C. (comme la messagerie électronique, les sessions sur les postes de travail, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiant, courriel, mot de passe).

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des utilisateurs. Ils ne doivent être communiqués à personne, ni responsable hiérarchique, ni informatique. Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit (hors fichier crypté). En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le S.I.C.

Lorsqu'ils sont choisis par l'utilisateur ([…] mot de passe), les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont élaborées par le service informatique en lien avec la direction afin de recommander les bonnes pratiques en la matière.

Aucun utilisateur ne doit se servir pour accéder au S.I.C. de l'établissement public d'un autre compte que celui qui lui a été attribué. Il ne doit pas non plus déléguer à un tiers les droits d'utilisation qui lui sont attribués.

L'authentification prévoit une restriction de l'accès au compte mise en place par le service de l'informatique interne (verrouillage du compte après 5 échecs).

Données

Chaque utilisateur est responsable pour ce qui le concerne du respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Les règles de confidentialité ou d'autorisation préalable avant diffusion externe ou publication sont définies par la direction et applicables quel que soit le support de communication utilisé.

L'utilisateur doit être particulièrement vigilant sur le risque de divulgation de ces informations dans le cadre d'utilisation d'outils informatiques, personnels ou appartenant à l'établissement public, dans des lieux autres que ceux de l'établissement public (hôtels, lieux publics…).

Poste de travail

L'établissement public met à disposition de l'utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions.

L'utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle.
- Connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par le service informatique.
- Déplacer l'équipement informatique (sauf s'il s'agit d'un Equipement ou Poste Nomade).
- Nuire au fonctionnement des outils informatiques et de communications.

Toute installation de logiciels supplémentaires est subordonnée à l'accord du service informatique.

Les postes de travails sont composés des éléments suivants :

- Poste fixe :
  - Unité centrale
  - Clavier / souris filaires
  - Ecran principal
  - *Option : Ecran secondaire en fonction des missions de l'utilisateur*
- Poste nomade :
  - Ordinateur portable + chargeur secteur
  - Ecran secondaire
  - Souris sans fil
  - *Option : Clavier filaire*
  - Sacoche ou sac à dos

Les demandes complémentaires justifiées par des missions spécifiques pourront être étudiées.

Messagerie

Chaque agent dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique normalisée attribuée par le service informatique.

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

Conseils généraux

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier postal : il obéit donc aux mêmes règles, en particulier en matière d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer à son supérieur.

Un message électronique peut être communiqué très rapidement à des tiers et il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du S.I.C., de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de l'établissement public et de l'utilisateur.

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d'informations à caractère confidentiel, ces vérifications doivent être renforcées ; en cas de besoin, un chiffrement des messages pourra être aussi proposé par le service informatique.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. De manière exceptionnelle, il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée (champ « CCI »), pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires (cas d'adresses email personnelles). En cas d'envoi à une liste de diffusion, il est important d'en vérifier les modalités d'abonnement, de contrôler la liste des abonnés et de prévoir l'accessibilité aux archives. Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes. Les messages importants doivent être envoyés avec un accusé de réception ou signés électroniquement.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent pas comporter d'éléments illicites, tels que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

La forme des messages professionnels doit respecter les règles définies par la direction, pour ce qui concerne la mise en forme et surtout la signature des messages.

En cas d'absence supérieure à 3 jours travaillés, l'agent doit mettre en place un répondeur automatique.

Limites techniques

Pour des raisons techniques, l'envoi de messages électroniques n'est possible, directement, que vers un nombre limité de destinataires, fixé par le service informatique. Cette limite est susceptible d'être levée temporairement ou définitivement sur demande adressée au service informatique, qui est aussi chargée de l'ouverture des listes de diffusion qui pourraient s'avérer nécessaires.

De même, le service informatique peut limiter la taille, le nombre et le type des pièces jointes pour éviter l'engorgement du système de messagerie. Privilégier la mention de liens permettant d'accéder aux documents. Pour des raisons de capacité mémoire, les messages électroniques sont conservés sur le serveur de messagerie pendant une durée maximale de deux ans. Passé ce délai, ils sont automatiquement supprimés. Si l'agent souhaite conserver des messages au-delà de ce délai, il lui appartient d'en faire des sauvegardes avec l'aide des procédures informatiques disponibles dans l'intranet. Il est aussi tenu de supprimer lui-même dès que possible tous les messages inutiles.

Utilisation personnelle de la messagerie

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte. Les messages envoyés doivent être signalés par la mention "*Privé*" ou "*Perso*" dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé de la même façon. Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé "Privé" ou "Perso". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Toutefois, les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'établissement public.

Utilisation de la messagerie par la délégation du personnel

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel, mais en utilisant la mention "Délégué" dans leur objet à l'émission et dans le dossier où ils doivent être classés.

Internet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par le service informatique qui est habilitée à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites.

Seule la consultation de sites ayant un rapport avec l'activité professionnelle est autorisée. En particulier, l'utilisation de l'Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives est strictement interdite. Il est aussi prohibé de créer ou mettre à jour au moyen de l'infrastructure de l'établissement public tout site Internet, notamment des pages personnelles en dehors de missions de l'utilisateur.

Bien sûr, il est interdit de se connecter à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de l'établissement public, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du S.I.C. de l'établissement public ou engageant financièrement celle-ci.

Tout téléchargement de fichier, en particulier de fichier média, est prohibé, sauf justification professionnelle dûment validée par la hiérarchie.

Ils sont informés que le service informatique enregistre leur activité sur Internet et que ces traces pourront être exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi, en particulier en cas de perte importante de bande passante sur le réseau de l'établissement public.

Téléphonie

Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un poste fixe et d'un terminal mobile, smartphone, tablette ou clé 4G. Pour ce qui est de l'utilisation des terminaux mobiles en connexion pour accès à des sites Internet ou à la messagerie électronique, les règles édictées ci-dessus s'appliquent de la même manière.

De plus, 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. Il est donc soumis aux mêmes règles rappelées plus haut.

Enfin, les connexions depuis l'étranger sont strictement interdites sauf autorisation exceptionnelle de la hiérarchie en cas d'urgence professionnelle.

Utilisation personnelle de la téléphonie

L'utilisation à caractère personnel du téléphone, fixe ou mobile, est tolérée, à condition qu'elle reste dans des limites raisonnables en termes tant de temps passé que de quantité d'appels. Les surcoûts pour l'établissement public 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 à des numéros surtaxés et des appels depuis l'étranger ou à destination de l'étranger, au sens de la facturation téléphonique.

Les utilisateurs sont informés que le service informatique enregistre leur activité téléphonique, aussi bien sur les postes fixes que sur les mobiles. Ces traces seront exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi. Toutefois, seule la direction pourra avoir accès aux numéros détaillés, permettant d'identifier les interlocuteurs d'un utilisateur, et seulement en cas de différend avec lui.

Cas spécifique du smartphone

L'utilisation de smartphones pour relever automatiquement 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 de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

Utilisateurs en télétravail

L'utilisateur en télétravail est soumis aux mêmes obligations que lorsqu'il travaille dans l'établissement public. L'exercice des missions d'un utilisateur en télétravail ne pourra se faire qu'au travers d'équipements appartenant à l'établissement public.

Dans le cas où l'utilisateur ne disposerais pas déjà d'un ordinateur portable, il se verra confier par le service informatique un kit de télétravail dans un délai de 10 jours ouvrés. Ce kit comprend notamment les éléments suivants :

- Une sacoche ou un sac à dos
- Une souris sans fil
- Un ordinateur portable

La première obligation du salarié est donc de prendre soin de l'équipement qui lui est attribué pour mener à bien ses missions.

L'ordinateur portable sur lequel l'utilisateur sera amené à réaliser ses missions est configurer de telle façons à ce qu'il puisse au travers d'un logiciel et d'un compte VPN nominatif (c'est-à-dire personnel et confidentiel) se connecter au réseau de l'établissement public afin d'accéder au différentes ressources mises à disposition.

Sécurité

Les règles de sécurité

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

- Signaler au service informatique toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.
- Ne jamais confier son identifiant / mot de passe à un tiers.
- Ne jamais demander son identifiant / mot de passe à un collègue ou à un collaborateur.
- Ne pas enregistrer ses mots de passe dans son navigateur sans mot de passe maître.
- Ne pas stocker ses mots de passe dans un fichier clair, sur un papier ou dans un lieu facilement accessible par d'autres personnes.
- Ne pas utiliser le même mot de passe pour des accès différents.
- Ne pas s'envoyer par courriel ses propres mots de passe.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramétrages du poste de travail.
- Ne pas installer de logiciels sans autorisation.
- Verrouiller son ordinateur dès qu'il quitte son poste de travail même pour un temps limité.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Effectuer des sauvegardes régulières de ses fichiers locaux sur un serveur de fichier.
- Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique et doit respecter les règles définies par l'établissement public.
- Ne pas mener d'actions engageant la responsabilité juridique ou financière de l'établissement public en répondant par exemple à un courriel.

<u>Règles de sécurité propres au smartphone :</u>

- N'installer que des applications nécessaires et vérifier à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques…). Il faut éviter d'installer les applications qui demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement.
- En plus du code PIN qui protège sa carte SIM, utiliser un schéma ou un mot de passe pour sécuriser l'accès à son terminal et le configurer pour qu'il se verrouille automatiquement.

En tout état de cause, l'Utilisateur doit séparer les usages personnels des usages professionnels :

- Ne pas faire suivre ses messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles.
- Ne pas héberger de données professionnelles sur ses équipements personnels (clés USB, téléphone…) ou sur des moyens personnels de stockage en ligne.
- Ne pas connecter des supports amovibles personnels (clés USB, disques durs externes…) aux ordinateurs de l'établissement public.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au S.I.C. de l'établissement public sans l'accord préalable du service informatique.

L'établissement public

L'établissement public met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du S.I.C.. À ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

Le service informatique est responsable de la mise en œuvre et du contrôle du bon fonctionnement du S.I.C.. Elle doit prévoir un plan de sécurité et de reprise du service, en particulier en cas de défaut matériel. Elle veille à l'application des règles de la présente charte. Elle est assujettie à une obligation de confidentialité sur les informations qu'elle est amenée à connaître.

La responsabilité de l'utilisateur

L'utilisateur est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence et de vigilance. En particulier, il doit signaler au service informatique toute violation ou tentative de violation de l'intégrité de ces ressources, et, de manière générale tout dysfonctionnement, incident ou anomalie. Sauf autorisation expresse de la direction et du service informatique, l'accès au S.I.C. avec du matériel n'appartenant pas à l'établissement public (assistants personnels, supports amovibles…) est interdit.

Dans le cas où il a été autorisé, il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité. De même, la sortie de matériel appartenant à l'établissement public doit être justifiée par des obligations professionnelles et nécessite l'accord exprès de la direction.

En cas d'absence, même temporaire, 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.

L'utilisateur doit effectuer des sauvegardes régulières des fichiers dont il dispose sur le matériel mis à sa disposition en suivant les procédures définies par le service informatique. Il doit régulièrement supprimer les données devenues inutiles sur les

espaces communs du réseau ; les données anciennes mais qu'il souhaite conserver doivent être archivées avec l'aide du service informatique.

L'utilisateur doit éviter d'installer ou de supprimer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques de sécurité au sein de l'établissement public. 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 l'établissement public. Il doit dans tous les cas en alerter le service informatique.

L'utilisateur s'oblige en toutes circonstances à se conformer à la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables. Il ne doit en aucun cas se livrer à une activité concurrente à celle de l'établissement public ou susceptible de lui causer un quelconque préjudice en utilisant le S.I.C..

Lors de périodes de télétravail l'utilisateur n'est pas autorisé à utiliser le matériel mis à disposition par l'établissement public à des fins personnelles ou en dehors des heures de travail.

Mesures de contrôle et Administration du S.I.C.

Afin de surveiller le fonctionnement et de garantir la sécurité du S.I.C., différents dispositifs sont mis en place.

Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information 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, messagerie instantanée type IRC etc.).

Les systèmes automatiques de traçabilité

Le service informatique opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du S.I.C. ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.

Il s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au S.I.C.. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l'évènement.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du S.I.C.. Sont notamment surveillées et conservées les données relatives :

- À l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers ;
- Aux connexions entrantes et sortantes au réseau interne, 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 ou le téléchargement de fichiers ;
- Aux appels téléphoniques émis ou reçus à partir des postes fixes ou mobiles pour surveiller le volume d'activités et détecter des dysfonctionnements.

Il est précisé que chaque utilisateur pourra avoir accès aux informations enregistrées lors de ces contrôles le concernant sur demande préalable à la direction. De plus, les fichiers journaux énumérés ci-dessus sont automatiquement détruits dans un délai maximum de 6 mois après leur enregistrement.

Procédure de contrôle manuel

En cas de dysfonctionnement constaté par le service informatique, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs.

Le contrôle concernant un utilisateur peut porter sur les fichiers contenus sur le disque dur de l'ordinateur, sur un support de sauvegarde mis à sa disposition ou sur le réseau de l'établissement public, ou sur sa messagerie. Alors, sauf risque ou

événement particulier, la direction ne peut ouvrir les fichiers ou messages identifiés par l'utilisateur comme personnels ou liés à la délégation de personnel conformément à la présente charte, qu'en présence de l'utilisateur ou celui-ci dûment appelé et éventuellement représenté par un délégué du personnel.

Gestion du poste de travail

A des fins de maintenance informatique, le service informatique peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur qui aura préalablement été informé de la finalité de l'opération.

Dans le cadre de mises à jour et évolutions du S.I.C., 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. Il s'interdit cependant d'accéder aux contenus du poste de travail.

Départ de l'utilisateur

Lors de son départ, l'utilisateur (ou son chef de service) doit restituer au service de l'informatique interne les matériels mis à sa disposition (hors poste de travail fixe qui doit rester sur place).

Il doit préalablement effacer ses fichiers et données privées. Toute copie de documents professionnels doit être autorisée par le chef de service.

Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum de 3 (trois) mois après son départ.

Information et sanctions

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque agent par voie électronique.

Le service informatique est à la disposition des agents pour leur fournir toute information concernant l'utilisation du S.I.C., en particulier sur les procédures de sauvegarde et de filtrage. Elle les informe régulièrement sur l'évolution des limites techniques du S.I.C. ainsi que sur les menaces susceptibles de peser sur sa sécurité. Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par le service informatique dans le cadre de la présente charte.

En cas de besoin, les agents pourront être formés par le service informatique pour appliquer les règles d'utilisation du S.I.C. prévues.

Le manquement aux règles et mesures de sécurité décrites dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des sanctions disciplinaires, des limitations ou suspensions d'utiliser tout ou partie du S.I.C., voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés. Dans ce dernier cas, les procédures prévues dans le règlement intérieur et dans le Code du travail seront appliquées. L'utilisation reconnue à des fins personnelles de certains services payants à travers le système de communication de l'établissement public donnera également lieu à remboursement de la part de l'utilisateur concerné.

Le président de la CCHLPP, se réserve également le droit d'engager ou de faire engager des poursuites pénales indépendamment des sanctions disciplinaires mises en œuvre, notamment en cas de fraude informatique, de non-respect des droits d'auteur ou de violation du secret des correspondances.

Entrée en vigueur

La présente charte est applicable à compter du 01/11/2021.

Elle a été adoptée après information et consultation :

- Des membres du bureau en date du 01/09/2021.
- Du Comité Technique en date du : 06/10/2021

Délibération du Conseil Communautaire en date du : 28/10/2021

ANNEXES

Liste des catégories de sites dont l'accès est restreint

Cette liste non exhaustive regroupe les catégories suivantes :

- Potentially Liable
  - Child Abuse
  - Extremist Groups
- Adult/Mature Content
  - Dating
  - Gambling
  - Pornography
  - Weapons (Sales)
- Bandwidth Consuming
  - Internet Radio and TV
  - Peer-to-peer File Sharing
- Security Risk
  - Dynamic DNS
  - Malicious Websites
  - Newly Observed Domain
  - Newly Registered Domain
  - Phishing
  - Spam URLs
- Local Categories
  - BlackList