Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

Syndicat Intercommunal des Technologies de l'Information pour les Villes

EXTRAIT DU REGISTRE DES DÉLIBÉRATIONS DU COMITÉ SYNDICAL

Séance du vendredi 12 avril 2024

N° CS_2024_04_5
Objet **: CHARTE INFORMATIQUE**
Date de convocation **: vendredi 05 avril 2024**
Date d'affichage du compte-rendu complet **: lundi 15 avril 2024**

Président de séance : Monsieur MILLET Pierre-Alain

Étaient présents (Titulaire(s) ou Suppléant(e)s) :

Monsieur MILLET Pierre-Alain,Monsieur VIOLLET Alain,Monsieur ARIAGNO Jeff,Monsieur BOUCHACOURT Jean-Luc,Monsieur MERMOURI Azdine,Monsieur GUICHARD Rhida,Monsieur SOW Abdoulaye,Monsieur MAILLET Eric

Étaient absents ou excusés et ayant donné pouvoir (Titulaires ou Suppléants) :

Madame VILLEDIEU Florence (donnant pouvoir à Monsieur BOUCHACOURT Jean-Luc)

Étaient absents ou excusés :

Monsieur RIAS Bernard,Monsieur MOULIN Guillaume,Monsieur BONY Vincent,Monsieur RAPP Florian,Monsieur BON Gaël

---

Le SITIV fournit un système d'information professionnel et sécurisé à l'ensemble de ses salariés.
Au regard du respect du Règlement Général sur la Protection des Données Personnelles (RGPD), toutes les administrations doivent mettre en place une charte informatique pour prévenir les risques encourus dans le cas du non-respect de ces règles et des obligations liées au RGPD.

La présente Charte informatique du SITIV, en annexe de la délibération, définit les conditions d'accès et les règles d'utilisation des moyens informatiques de l'établissement. 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. 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 de l'établissement.
La charte informatique donne un cadre pour définir un comportement responsable et un bon fonctionnement pour tous, en décrivant tous les moyens nécessaires pour contrôler et assurer la protection des personnes et du SITIV, en fonction des risques encourus par l'agent et l'employeur, ainsi que les contraintes légales.

La présente charte, recueil de règles législatives, réglementaires, de déontologie et de sécurité a pour objet :

- De définir l'ensemble des bonnes pratiques d'utilisation des ressources informatiques et de communication,
- De préserver l'intérêt de chacun et l'intérêt général,
- De préserver un environnement de travail professionnel,
- De garantir l'intégrité du système informatique,
- De protéger les informations qui sont la propriété du SITIV
- De limiter les risques de recherche de responsabilités pénales et civiles de chacun.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

La charte s'impose aux personnels de l'établissement, toutes catégories confondues. Cette charte et ses principes associés s'imposent également aux prestataires et services extérieurs utilisateurs ou ayant simplement accès aux technologies du SITIV.
Pour les salariés assurant des fonctions d'administrateurs de systèmes, une charte renforcée vient compléter et préciser un certain nombre d'obligations.

LE COMITÉ SYNDICAL, APRÈS EN AVOIR DÉLIBÉRÉ,

A L'UNANIMITÉ DES SUFFRAGES EXPRIMÉS AVEC :

9 VOIX POUR

DÉCIDE

- De valider la charte informatique ci-annexée
- De validet la charte informatique administrateur ci-annexée

Ainsi fait et délibéré les jours, mois et an susdits et ont signé les membres présents.

Pour expédition certifiée conforme,

Signé par : Pierre Alain MILLET
Date : 12/04/2024
Qualité : Présidence du SITIV

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

CHARTE INFORMATIQUE

Table des matières

1. Préambule 3
2. Le champ d'application 4
2.1. Le système d'information et communication 4
2.2 Les utilisateurs 5
2.2.1 – Les visiteurs 6
2.2.2 – Les administrateurs 6
3. Conditions générales d'utilisations 7
3.1 Confidentialité 7
3.1. Sécurité 7
3.2. Utilisation à des fins personnelles 10
3.3. Protection et propriété des données produites par les utilisateurs 12
4. Internet 13
5. Messagerie électronique 14
5.1. Mise à disposition 14
5.2. Règles d'utilisation 14
5.2.1. Utilisation professionnelle 14
5.2.2. Utilisation personnelle 15
5.2.3. Sécurité et filtrage 15
6. Les réseaux sociaux, blogs et forums 17
7. Téléphonie et smartphone fournis par le SITIV 18
8. Droit à la déconnexion 19
9. Photocopieurs et scanners 20
10. Données personnelles 21
11. Contrôle des activités 24
12. Information et sanctions 25
13. Entrée en Vigueur 27
14. Annexes 28
13.1 La Réglementation 28
14.1. Le Droit Disciplinaire 28
14.2. Le Code Pénal 29
14.3. Le Code Civil 31
14.4. Contacts utiles 31

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

1. Préambule

Le SITIV met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des outils mobiles.

Le SITIV s'engage à :

- Mettre à disposition les ressources informatiques matérielles et logicielles nécessaires au bon déroulement de la mission des utilisateurs.
- Mettre en place des programmes de formation adaptés et nécessaires aux utilisateurs pour une bonne utilisation des outils.
- Informer les utilisateurs des diverses contraintes d'exploitation (interruption de service, maintenance, modification de ressources…) du système d'information susceptibles d'occasionner une perturbation.
- Effectuer les mises à jour nécessaires des matériels et des logiciels composant le système d'information afin de maintenir le niveau de sécurité en vigueur dans le respect des règles d'achat et des budgets alloués.
- Respecter la confidentialité des "données utilisateurs" auxquelles il pourrait être amené à accéder pour diagnostiquer ou corriger un problème spécifique.

La vocation de notre charte informatique réside dans l'encadrement de l'utilisation des moyens informatique mis en place par notre service public le « Syndicat Intercommunal des Technologies de l'Information pour les Villes » (SITIV) en tant qu'employeur, enregistré au SIREN 256 910 183 et représenté par son Président.

Ces objectifs se déclinent comme suit :

- Sensibiliser les utilisateurs aux risques et conséquences d'une action volontaire ou involontaire pouvant compromettre le système d'information tels que :
  - Risque de piratage/attaque informatique
  - Utilisation abusive des ressources de l'entreprise
  - Détention et/ou diffusion d'informations et/ou de données protégées par la loi
  - Préjudice à l'image du Syndicat
- Informer les utilisateurs sur les modalités d'utilisation des ressources informatiques.
- Définir les sanctions disciplinaires en cas de manquement à cette même charte.
- Dans le cadre de la loi, informer des contrôles effectués par le syndicat.

2. Le champ d'application

2.1. Le système d'information et communication

La présente charte s'applique au système d'information et de communication du SITIV, notamment constitué d'un ensemble "matériels - système d'exploitation - logiciels" mis à disposition des utilisateurs :

- Matériel informatique et téléphonique :
  - Unités centrales, écrans, claviers, souris, casque etc. qu'ils s'agissent d'ordinateurs (fixes ou portables), périphériques y compris clés USB, disques durs externes…
  - Imprimantes, photocopieurs, scanners, fax
  - Téléphones, smartphones, tablettes et clés 4G
- Système d'exploitation et logiciels :
  - Windows, Linux, macOS, androïd…,
  - Logiciels : pack bureautique, logiciels de gestion, applications spécifiques,
  - Abonnements à des services interactifs,
  - Système de messagerie, réseaux sociaux
- Réseau informatique et infrastructures :
  - Serveurs, routeurs, firewall et connectique,
  - Connexion internet, intranet, extranet, wifi, cloud

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des salariés connecté au réseau du SITIV, ou contenant des informations à caractère professionnel concernant le SITIV.

À défaut de qualification explicite, le patrimoine de données des Villes adhérentes du SITIV, des membres de l'entente TNO et/ou des partenaires auxquels le SITIV et ses utilisateurs/collaborateurs ont accès dans le cadre de l'exercice de leurs activités sont considérées comme interne et sont à ce titre confidentiel.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

2.2 Les utilisateurs

Sauf indication contraire, les directives énoncées dans cette charte sont applicables à la totalité des utilisateurs, des données et des systèmes d'informations et de communication du SITIV, à distance ou en présentiel et ceux sans distinction de statut et de temporalité (stagiaires, agents, invités, etc.)

Elle s'applique également à tout partenaire ou prestataire extérieur ayant accès aux données et aux outils informatiques du SITIV.

Chaque utilisateur doit adopter une attitude responsable et respecter les règles définies sur l'utilisation des ressources et notamment :

- Prendre soin des outils de travail fournis par le SITIV et s'engage à les restituer à son départ.
- En cas de perte, de vol ou de détérioration d'une ressource signaler l'incident le plus rapidement possible au service Hébergement/Infrastructure.
- Ne pas masquer son identité, ni usurper l'identité d'autrui, ni prêter son compte. Respecter les règles relatives à l'identification et l'authentification, sachant qu'il est interdit d'utiliser le compte ou s'authentifier en tant qu'un autre utilisateur.
- S'assurer de l'intégrité et la confidentialité des données et ne pas perturber la disponibilité du système d'information.
- Ne pas stocker ou transmettre d'informations portant atteinte à la dignité humaine, ni envoyer ou transférer des messages dont le contenu est irrespectueux, provocant, injurieux, dégradant, malveillant, menaçant, et en règle générale, dont le contenu est contraire aux bonnes mœurs.
- Ne pas marquer les données exploitées d'annotations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et images de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée
- Respecter le droit de propriété intellectuelle : non reproduction et/ou non diffusion de données soumises à un droit de copie non-détenu, interdiction de copie de logiciel sans licence d'utilisation
- Ne pas porter atteinte à la sécurité du système d'information par l'utilisation de "ressources extérieures" matérielles ou logicielles
- Respecter les contraintes liées à la maintenance du système d'information.

- Prendre connaissance et appliquer pour ses usages l'ensemble des prescriptions de la PSSI et de ses annexes.

2.2.1 – Les visiteurs

Les personnes extérieures, de passage dans les locaux et sites du SITIV, pourront bénéficier, pour leurs équipements personnels, d'un accès réseau internet « invités ». Cet accès « invité » sera rendu accessible par le service Infrastructure et Hébergement selon les modalités techniques mise en œuvre par le SITIV.

Une trace du trafic sur ce réseau « invité » pourra être faite dans le but d'identifier d'éventuels incidents de sécurité ou d'exploitation.

Le SITIV ne peut être tenue responsable d'éventuels dommages sur les équipements personnels, lors d'une utilisation « réseau invité ».

2.2.2 – Les administrateurs

Les administrateurs du système d'information et communication veillent au bon fonctionnement du système, à sa disponibilité, sa maintenance, sa sécurité et son évolution pour répondre aux mieux aux besoins du SITIV.

Ils mettent en œuvre toutes les procédures et ressources nécessaires afin d'apporter services et supports aux utilisateurs.

En fonction de leur champ d'activité et de responsabilité, les administrateurs du système d'information et communication, sont soumis au secret professionnel et ne peuvent divulguer des informations à caractère personnel ou privé, auxquelles ils pourraient avoir accès dans le cadre de leur missions et fonctions.

3. Conditions générales d'utilisations

3.1 Confidentialité

Tout utilisateur dispose d'un droit d'accès au système d'information et communication. Ce droit d'accès est unique et personnel.

Les droits d'accès et d'utilisation du système d'information et communication du SITIV sont donnés par les administrateurs. Ces droits sont limités aux activités exercées pour le SITIV et disparaissent lorsque l'utilisateur quitte le syndicat ou que la mission du prestataire prend fin.

Ces droits d'accès peuvent être suspendus, si le comportement d'un utilisateur n'est pas compatible avec les règles énoncées dans la présente charte, ou pour des raisons de sécurité.

Lors de la première utilisation des identifiants (login/mot de passe) l'utilisateur devra modifier son mot de passe qui lui a été communiqué par le service Hébergement & Infrastructure, par un mot de passe personnel, qu'il s'engage à ne pas divulguer et qui devra respecter le degré de complexité défini par le SITIV dans le cadre de sa PSSI.

Pour certaines applications ou supports nécessitant un identifiant et/ou un mot de passe distinct, l'utilisateur devra privilégier l'utilisation du coffre-fort à mots de passe mis à disposition par le SITIV.

L'utilisateur ne doit pas prendre, modifier ou tenter de déchiffrer le mot de passe d'un autre utilisateur.

3.1. Sécurité

Les attaques informatiques ou une mauvaise utilisation de ces outils peuvent avoir des conséquences extrêmement graves.
En effet, ils augmentent les risques d'atteinte à la confidentialité, de mise en jeu de la responsabilité, d'atteinte à l'image, à la réputation, à l'intégrité et à la sécurité des fichiers, des données personnelles (virus, intrusions sur le réseau interne, vols de données).
Les outils informatiques peuvent aussi être une source de perte de productivité et de coûts additionnels.
Le SITIV met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et communication.

A ce titre, les accès aux ressources sensibles sont limités. Le service Hébergement est responsable de la mise en œuvre et du contrôle du bon fonctionnement du système d'information et de communication et 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.
L'utilisateur est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions et missions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence et de vigilance, à savoir :

- En cas d'absence momentanée, même très courte l'utilisateur doit :
  - Verrouiller son PC (Ex. : maintenir enfoncées les touches 'Ctrl+Alt+Suppr' ou « Touche drapeau Windows L » et cliquer sur 'Verrouiller l'ordinateur'), en cas d'oubli un verrouillage automatique se mettra en place.
  - L'utilisateur doit quitter logiciels métiers (déconnexion) et verrouiller son PC.

- A la fin de sa journée de travail, l'utilisateur doit quitter les applications, arrêter le système par arrêt logiciel, le poste de travail et éteindre l'écran.

- Un premier niveau de sécurité consiste à utiliser des mots de passe sûrs non communiqués à des tiers et régulièrement modifiés (une fois par an).

- La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde quotidienne des informations sur les serveurs et non le disque local.

- L'utilisateur doit signaler tous dysfonctionnements ou anomalies à la hiérarchie et au RSI. *(exemple : un tiers non autorisée se rendant compte qu'il a accès à des informations confidentiel via son compte utilisateur)*
- L'utilisateur doit signaler au RSSI toute violation ou tentative de violation suspectée de son compte utilisateur.

- L'utilisateur doit procéder régulièrement à l'élimination des fichiers non- utilisés et à l'archivage, dans le but de préserver la capacité de mémoire, et selon les règles d'archivage légal.

- L'usage des supports amovibles (CD, clé USB, etc.) est interdit.

- L'utilisateur ne doit pas supprimer ou désactiver ou chercher à contourner les mesures de sécurité (antivirus, firewall et autres) installées sur les équipements locaux, distants ou sur toute partie du système d'information et communication du SITIV.

- L'utilisateur doit être particulièrement vigilant lors de l'envoi d'informations sensibles sur les moyens de communication non sécurisés : SMS, messagerie électronique ou Internet.

- Dans le cadre de ses activités professionnelles, l'utilisateur ne doit utiliser que les matériels mis à disposition par le SITIV pour se connecter au système d'information.

- L'utilisateur s'interdit toute installation de logiciel non nécessaire à l'exécution de ses missions et/ou non validé par la collectivité.

La signature électronique (loi n° 2000-230 du 13 mars 2000) est présumée fiable jusqu'à preuve du contraire. Son utilisation est limitée aux personnes autorisées et doit respecter la procédure définie par le SITIV.

3.2. Utilisation à des fins personnelles

L'utilisation des équipements informatiques (matériels et logiciels), numériques et téléphoniques du SITIV est limitée à un usage professionnel.

Durant les heures de travail, il est toléré un usage modéré et très occasionnel, à condition que cela n'entrave pas l'activité professionnelle (la sienne et celle de ses collègues) de :

- L'accès à Internet pour des besoins personnels
- Un usage ponctuel du téléphone pour des communications personnelles locales (une attention particulière est demandée en cas d'appel sur des numéros surtaxés). Le SITIV peut procéder au contrôle de l'ensemble des appels émis.

En dehors des heures de travail, cette utilisation à titre privé est acceptée, sous réserve qu'elle ne perturbe pas l'activité professionnelle du service, ni ne porte atteinte à l'image du SITIV.

Le SITIV se réserve le droit de restreindre ou suspendre temporairement cette utilisation privée, sans préavis en cas de danger pour le système d'information.
Tout utilisateur ayant une utilisation abusive des moyens informatiques (accès à des sites web non professionnels, impression de documents personnels, minage de cryptomonnaie, p2p…), numériques ou téléphoniques sera averti, puis éventuellement sanctionné.
Le SITIV se réserve ainsi la possibilité d'avoir des relevés d'usages de son système d'information et communication. Si une anomalie est constatée, un relevé détaillé des consommations du poste pourra être demandé ainsi que des explications auprès du titulaire du poste.

Les données personnelles de l'utilisateur, qu'il s'agisse de fichiers ou d'autres types de données, doivent être clairement identifiées en utilisant les termes « Privé » ou « Perso » ou « Personnel » dans leurs noms et/ou celui du répertoire les stockant, et/ou dans le nom du disque réseau, qui devra être désigné comme « P:\».

Afin d'éviter toute confusion, il ne faut en aucun cas mettre la mention « CONFIDENTIEL »

Les messages envoyés doivent être signalés également par la mention « Privé » ou « Personnel » dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé « Privé » ou « Personnel ».
Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé « Privé » ou « Personnel ».

En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Les données, fichiers et messages électroniques expressément désignés comme personnels ou privés par un utilisateur ne seront accessibles par le SITIV qu'en présence de l'utilisateur ou en cas de risques majeurs portant atteinte au système d'information et communication.

En cas de manquement de désignation du caractère personnel ou privé des messages, ceux-ci sont présumés être à caractère professionnel.

En cas de départ d'un utilisateur, l'ensemble des données personnelles ou privées qu'il laisserait dans le système d'information et communication du SITIV serait détruit dans un délai maximum d'un mois après son départ.

Par ailleurs, l'utilisateur ne doit pas effectuer de copie de logiciel. En effet, l'utilisation et la diffusion de logiciels acquis illégalement et en irrespect du Code de la Propriété Intellectuelle (loi 92-597) constituent un délit de contrefaçon passible d'amende et d'emprisonnement.

3.3. Protection et propriété des données produites par les utilisateurs

Au SITIV, le travail sur le réseau constitue une règle qui s'impose à tous.
En effet, seuls les fichiers enregistrés sur le réseau font l'objet d'une sauvegarde générale et quotidienne.
Travailler sur le réseau constitue donc, pour tous, un impératif de sécurité et de conservation des données.
Les archives de chaque utilisateur constituent la mémoire du SITIV et garantissent la continuité d'activité. Cela signifie en particulier :

- Que les collaborateurs ne travaillent pas en individualité mais pour le compte du SITIV qui les emploie. Ils ne sont donc pas « propriétaire » de leur travail. Leurs documents et fichiers informatiques doivent être correctement nommés, de manière normative, voire datée, classés en arborescence par dossiers et sous dossiers, de manière thématique et non personnalisée et organisés comme doivent l'être les dossiers physiques ;
- Le travail en local sur disque « C » est à éviter, car il ne fait pas l'objet d'une sauvegarde.

4. Internet

Dans le cadre de leur activité, les Utilisateurs ont accès à internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé.

L'utilisateur s'engage lors de ses consultations Internet à ne pas se rendre sur des sites portant sur des sujets pénalement répréhensibles (pédopornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée…).

Le téléchargement, en tout ou partie, de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux ou films, logiciels propriétaires, etc.) est strictement interdit.

De même, le visionnage de films et l'écoute de musique en streaming, non liés à l'activité professionnelle ne sont pas autorisés.

Le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet est interdit.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

5. Messagerie électronique

5.1. Mise à disposition

Le SITIV met à disposition aux utilisateurs des adresses électroniques, la majorité, sauf cas particuliers[1], suivent la politique de nommage suivante : 1ère lettre du prénom de l'utilisateur, suivi du son nom@sitiv.fr.

(¹ pour exemple : adresse de contact utile tel que securite-si@sitiv.fr, impossibilité d'appliquer la politique de nommage car adresse déjà existante, etc.)

L'utilisation de la messagerie est principalement réservée à des fins professionnelles. Dans ce cadre, cette messagerie est donc susceptible d'être ouverte par les administrateurs afin de garantir une sécurité du système, une continuité de service… Cette démarche ne sera mise en œuvre qu'après validation de la direction générale, suite à la demande du responsable de service ou avec l'accord formel de l'utilisateur.

Pour le partage de fichiers, l'utilisateur privilégiera la plateforme collaborative ou serveur partagé, mis à disposition par le SITIV (type cloud).

5.2. Règles d'utilisation

5.2.1. Utilisation professionnelle

L'utilisateur s'engage à ne pas envoyer en dehors des services du SITIV des informations professionnelles nominatives ou confidentielles, sauf si cet envoi est à caractère professionnel et autorisé par son supérieur hiérarchique.

L'utilisateur soigne la qualité des informations envoyées à l'extérieur et s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine, à la vie privée, aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.

L'utilisateur signera tout courriel professionnel.

Il doit vérifier la liste des destinataires. Il doit également vérifier le contenu et l'historique des messages transférés (gestion du "Répondre à tous").

L'utilisateur doit éviter de surcharger le réseau d'informations inutiles, par exemple en évitant de mettre automatiquement des accusés de réception et de lecture de mails. Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier « éléments supprimés » doit être vidé périodiquement.

En cas d'absence prévisible, l'utilisateur devra mettre en place un message automatique d'absence indiquant la date de retour prévue et invitant le correspondant à rediriger son mail vers un agent ou l'adresse générique du service qui pourra gérer les messages et demandes pendant son absence.

En cas d'absence non prévisible, l'administrateur pourra, si nécessaire, ajouter un message d'absence réorientant vers une autre adresse mail et de préférence une adresse mail générique.

5.2.2. Utilisation personnelle

Les courriers à caractère privé et personnel doivent expressément porter la mention « personnel » ou « privé » ou « perso » dans leur objet ou être classés dans un dossier spécifique « personnel » ou « privé » ou « perso ».

Afin d'éviter toute confusion, il ne faut en aucun cas mettre la mention « CONFIDENTIEL » en objet d'un message personnel, le terme « confidentiel » pouvant être utilisé dans le domaine professionnel.

En cas de manquement à ces règles, les courriers sont présumés être à caractère professionnel.

Pour réduire le risque d'utilisation abusive, l'adresse e-mail étant attribué à l'utilisateur ne doit pas être utilisée pour s'identifier ou s'inscrire sur des forums, réseaux sociaux, messageries instantanées, sites d'achats et autres sites sans rapport avec l'activité professionnelle.

5.2.3. Sécurité et filtrage

L'utilisateur doit veiller à ne pas ouvrir les courriels dont le sujet paraîtrait suspect. Ces messages peuvent contenir des programmes malveillants dont potentiellement des systèmes de cryptage de fichiers, appelé cryptoLocker et/ou ransomwares qui est en fait un logiciel malveillant pouvant se propager.

Enfin, un mécanisme de filtrage des mails entrants a été mis en place permettant ainsi de supprimer les mails non sollicités (SPAM) et/ou représentant des menaces pour le système d'information et communication du SITIV.

Les filtres d'entrée des courriers indésirables permettent d'économiser les ressources informatiques du SITIV tant en termes de réseau que de stockage, et de protéger les utilisateurs contre certains types de menaces.

Les utilisateurs ont la possibilité de consulter la liste des mails envoyés à leur adresse et rejetés par le système. Ils peuvent constituer leurs propres listes blanches et listes noires d'expéditeurs à autoriser ou interdire expressément.

Les mails sortants sont également analysés par un antivirus pour éviter la propagation.

6. Les réseaux sociaux, blogs et forums

L'utilisation des réseaux sociaux est réservée à des fins professionnelles.

De manière générale, toute publication d'information interne, financière, stratégique et/ou confidentielle du SITIV sur les réseaux sociaux, blogs ou forums est interdite.

Des autorisations de communication sur les réseaux sociaux, blogs ou forums sont attribuées aux collaborateurs, aux services, qui sont habilités à parler au nom du SITIV. La distinction entre l'utilisation professionnelle et l'utilisation personnelle est imposée (création de deux profils).

Les utilisateurs doivent veiller au respect des lois et règlements en vigueur et par conséquent, ils ne doivent pas faire de commentaires injurieux, diffamatoires ou racistes, et respecter les lois relatives à la propriété intellectuelle et notamment le droit d'auteur et le droit à l'image.

Les utilisateurs sont personnellement responsables des contenus ou commentaires publiés sur les réseaux sociaux, blogs et forums.

Par ailleurs, il est rappelé, au titre des droits et obligations des fonctionnaires (discrétion professionnelle, devoir de réserve et devoir de neutralité), que la liberté d'expression sur les réseaux sociaux, blogs et forums n'est pas sans limite pour l'utilisateur (agent titulaire ou contractuel). L'utilisateur doit respecter les obligations déontologiques, même en dehors du service.

En effet, lorsqu'il s'exprime publiquement sur les réseaux sociaux, blogs ou forums soit à titre personnel soit au titre d'autre qualité comme celle d'une association, l'utilisateur ne doit pas faire état de sa qualité au sein de l'établissement.

L'utilisateur doit ainsi éviter toute manifestation d'opinion de nature à porter atteinte à l'image du SITIV. Enfin, l'utilisateur s'engage à ne pas alimenter de polémique et/ou écrire des textes contraires à la bien séance et/ou à la loi dans un site de type « réseau social » (Facebook, Twitter, LinkedIn etc…) un site type « blogs » ou « forum » avec son adresse mail professionnelle, ni de poster des vidéos, des fichiers, des programmes contraires à la bien séance et/ou à la loi.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

7. Téléphonie et smartphone fournis par le SITIV

L'utilisation des téléphones fixes et portables fournis par le SITIV est réservée à des fins professionnelles.

Le smartphone est un outil de travail dont l'usage personnel peut être autorisé (mention "personnel" pour messages personnels)

Il n'est pas attendu de répondre aux appels ou aux mails en dehors du temps de travail (soir, week-end et congé.)

Il est rappelé que l'usage de téléphone portable n'est pas autorisé en conduisant, sauf véhicule équipé en Bluetooth et ceci de manière très occasionnelle.

En cas d'absence, l'utilisateur doit effectuer un renvoi sur le poste d'un autre agent du service ou sur l'accueil téléphonique. L'agent qui quitte définitivement le SITIV doit restituer le téléphone portable professionnel.

L'utilisation des téléphones portables personnels doit rester limitée, occasionnelle et discrète (appels et sms). Il ne doit pas venir perturber une réunion ou un entretien.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

8. Droit à la déconnexion

L'utilisation des Technologies de l'Information et de la Communication mis à disposition des salariés, doit respecter leur vie personnelle. A cet égard, ils bénéficient d'un droit à déconnexion les soirs, les weekends et pendant leurs congés, ainsi que l'ensemble des périodes de suspension de leur contrat de travail, sauf circonstances exceptionnelles.

Ce droit à la déconnexion consiste à éteindre et/ou désactiver les outils de communication mis à leur disposition comme le téléphone portable, l'ordinateur portable et la messagerie électronique professionnelle en dehors des heures habituelles de travail. Les salariés pourront même durant leurs temps de repos laisser ces outils au sein de la société en ayant informé parallèlement leur supérieur hiérarchique.

L'entreprise précise que les salariés n'ont pas l'obligation, hors plages de travail habituelles, en particulier, en soirée, les week-ends et lors de leurs congés, de répondre aux courriels et appels téléphoniques qui leur sont adressés. Il leur est demandé également, pendant ces périodes, de limiter au strict nécessaire et à l'exceptionnel l'envoi de courriels ou les appels téléphoniques.

9. Photocopieurs et scanners

L'utilisateur s'oblige à respecter des règles d'économie et de non-gaspillage concernant l'usage des imprimantes et des photocopieurs. Ainsi, à l'ère de la dématérialisation, il est recommandé de n'imprimer que les documents qui le nécessitent, de préférer le recto verso et l'impression couleur doit rester une exception.

L'utilisateur est invité à aller récupérer ses impressions et utiliser des copieurs à code d'accès pour les impressions de documents sensibles comprenant des informations confidentielles. L'utilisateur veillera donc à ne pas oublier des documents papiers en attente dans les copieurs en accès libre ou public.

Concernant la numérisation de document, il est conseillé de scanner au format PDF compact et d'enregistrer directement le dossier scanné sur le serveur, ce qui pourra permettre de partager des fichiers via un cloud.

L'utilisation des moyens de reprographie à des fins personnelles est strictement interdit.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

10. Données personnelles

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, complétée et renforcée par le règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractères personnel et à la libre circulation de ces données (RGPD) définit les conditions dans lesquelles des traitements de données personnels peuvent être opérés.
Elle institue au profit des personnes concernées par les traitements des droits que la présente charte informatique invite à respecter, tant à l'égard des utilisateurs que des tiers.

Des traitements de données automatisés et manuels sont effectués dans le cadre des systèmes de contrôle, prévus dans la présente charte. Ils sont, en tant que de besoin, déclarés conformes.

Tout utilisateur pourra avoir accès aux données le concernant et ces données ne seront conservées que sur une période maximale définie au regard de la finalité du traitement, de la licéité du traitement...

Il est rappelé aux utilisateurs que les traitements de données à caractère personnel doivent être conforme au RGPD.
Les utilisateurs souhaitant réaliser, dans le cadre professionnel, des traitements relevant dudit règlement sont invités à prendre contact avec la déléguée à la protection des données à l'adresse securite-si@sitiv.fr.

En effet, toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclaré auprès du Délégué à la Protection des données personnelles du SITIV, qui étudie :

- La pertinence des données recueillies.
- La finalité du traitement.
- Les durées de conservation prévues.
- Les destinataires des données.
- Le moyen d'information des personnes fichées et les mesures de sécurité à déployer pour sécuriser les données.

Tout utilisateur est tenu d'assurer la protection des données à caractère personnel qu'il traite dans le cadre de ses fonctions notamment en :

- Protégeant les codes d'accès aux applications et systèmes d'information qu'il utilise,

- En limitant strictement aux besoins de son activité la diffusion par des moyens informatiques ou autre (impressions papier par exemple) des données à caractère personnel en sa possession,
- En ne conservant pas ces données au-delà de la durée nécessaire au traitement auquel elles sont destinées.

L'utilisateur s'engage à :

- Ne pas utiliser les données à des fins autres que celles prévues par ses attributions ;

- Ne divulguer ces données qu'aux personnes dûment autorisées, qu'il s'agisse de personnes privées, publiques, physiques ou morales ; Les données à caractère personnel relevant de la vie privée des personnes et, collectées par un utilisateur, ne peuvent être communiquées à des tiers et ne seront donc pas publiable, sont notamment concernées les données au titre de : l'état civil, la situation patrimoniale et financière, la domiciliation bancaire la qualité de travailleur handicapé, la formation initiale, les horaires de travail, les sympathies politique et l'appartenance à un parti politique, les croyances religieuses. A l'inverse d'autres données ne sont couvertes par le secret de la vie privée, notamment les données dont on estime que les usagers doivent avoir connaissance, soit au titre de l'organisation du service public, soit afin de pouvoir exercer pleinement un droit de recours (bénéficiaire d'une autorisation d'urbanisme, informations librement consignées sur des registres d'enquête publique…).

- S'assurer que seuls des moyens de communications sécurisés seront utilisés pour transférer ces données ;

- 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 pour préserver la sécurité physique et logique de ces données.

- Prévoir des mesures techniques et organisationnelles pour protéger les données (destruction, perte, altération, diffusion ou accès non autorisés, etc.). Ces mesures doivent assurer un niveau de sécurité approprié aux risques et à la nature des données considérées.

Concernant les archives courantes et intermédiaires, elles relèvent du régime de droit commun du RGPD et de la loi Informatique et liberté, c'est à dire le droit à l'effacement, modification, opposition, portabilité…. Ces droits sont toutefois limités dans certains cas, comme par exemple le droit à l'effacement qui ne s'applique pas lorsqu'il s'agit de respecter une obligation légale ou pour exécuter une mission d'intérêt public.

Concernant les archives définitives, le RGPD et l'article 36 de la loi Informatique et libertés confirment la possibilité de conserver les données au-delà de la durée de conservation prévue dans le traitement initiale, à des fins archivistiques dans l'intérêt publics, à des fins de recherches scientifique ou historique ou statistiques.
Lorsqu'il sera question de supprimer des données à caractère personnel, l'utilisateur est invité à prendre attache auprès du Délégué à la Protection des Données du SITIV.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

11. Contrôle des activités

Les administrateurs du système d'information et communication du SITIV sont amenés à prendre toutes dispositions nécessaires pour assurer le bon fonctionnement des réseaux et moyens informatiques du SITIV et le respect de la présente charte informatique. Des contrôles techniques peuvent ainsi être opérés :

- Dans un souci de sécurité du réseau et/ou des ressources informatiques, de maintenance et de gestion techniques, de respect de la législation applicable et notamment de respect des règles relatives à la protection de la vie privée ;

- Dans un souci de vérification de l'utilisation des moyens informatiques et des télécommunications afin qu'elles restent conformes aux règles édictées par la présente charte.

- Dans un souci de recherche de preuves dans le cadre d'une action judiciaire et/ou d'une atteinte au RGPD, en déclenchant une investigation numérique. Les administrateurs du système d'information et communication disposent d'outils permettant d'analyser tout ce qui transite par celui-ci et grâce aux logs des systèmes peuvent connaître les actions réalisées (sachant que cette liste n'est pas exhaustive) :

- Les connexions au réseau (identifiants, dates et heures de connexion…),

- Les fichiers stockés sur les serveurs (format, date création ou de dernière modification, taille…)

- Les connexions passant par Internet (identifiants de connexion, sites visités, volumes de données transférées, dates et heures de connexion…).

Ces logs sont enregistrés durant une année pour permettre la détection de comportements malveillants ou contraires aux politiques de sécurité du SITIV, de dysfonctionnements du système d'information, l'analyse a posteriori d'incidents de sécurité, pour se conformer aux textes et règlements en vigueur, ainsi que pour contrôler le respect de la présente charte.

Elles peuvent être communiquées aux autorités publiques compétentes en cas de réquisition judiciaire, aux conseils juridiques et également aux services de ressources humaines du SITIV.
Les administrateurs du système d'information et communication sont équipés d'outils permettant une prise en main à distance des postes, des logiciels… Cette prise en main ne s'effectue qu'en présence de l'utilisateur en poste ou avec son accord.
Le contenu même des échanges réalisés par les utilisateurs n'est pas conservé.

12. Information et sanctions

La présente charte est annexée au règlement intérieur. A compté du 12/04/2024, soit l'entrée en vigueur de la présente charte, chaque utilisateur du SITIV s'en verra remettre un exemplaire, il devra en prendre connaissance et devra s'engager à la respecter. Chaque agent sera tenu informé des adaptations via les voies de communication internes.

Les collaborateurs du service hébergement sont à la disposition des utilisateurs pour leur fournir toute information concernant l'utilisation du système d'information et communication, en particulier sur les procédures de sauvegarde et de filtrage.

Elle les informe régulièrement sur l'évolution des limites techniques du système d'information et de communication 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 hébergement dans le cadre de la présente charte.

L'utilisateur ne doit à aucun moment oublier qu'il vit et travaille au sein d'une collectivité. Il s'interdit toute utilisation abusive d'une ressource commune.

Il s'interdit également de perturber tout autre utilisateur du système d'information et communication à l'aide d'outils électroniques, de masquer son identité ou de s'approprier le mot de passe d'un autre utilisateur.

Il s'interdit également de porter atteinte à l'intégrité d'un autre utilisateur, notamment par l'intermédiaire de messages et d'images provocantes. Il s'interdit enfin de saturer la messagerie des autres utilisateurs par l'envoi de messages, trop nombreux ou trop volumineux, non liés à l'activité professionnelle.

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 avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Dans ce dernier cas, les procédures prévues dans le cadre des statuts de la fonction publique seront appliquées. L'utilisation reconnue à des fins personnelles de certains services payants à travers le système de communication donnera également lieu à remboursement de la part de l'utilisateur concerné.

Le SITIV 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 ou de violation du secret des correspondances.
Le manquement à la présente charte pourrait entraîner le retrait du droit d'utilisation d'un outil, d'une application ou d'un matériel informatique/téléphonique et/ou des mesures d'ordre disciplinaire et/ou des sanctions pénales.

Le niveau de sanction sera proportionnel à la faute commise et sera apprécié au regard du manquement aux obligations professionnelles et de la présente charte.

13. Entrée en Vigueur

La présente charte est applicable à compter du 12 Avril 2024.

14. Annexes

L'agent doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par l'ordonnance n°2021-1574 du 24 novembre 2021 portant droits et obligations des fonctionnaires et l'ordonnance n°2021-1574 du 24 novembre 2021 relative à la fonction publique territoriale.

13.1 La Réglementation

- Loi n° 78-17 du 06/01/1978 sur l'informatique, les fichiers, les libertés.
- Loi n° 78-753 du 17/07/1978 sur la liberté d'accès aux documents administratifs.
- Loi n° 85-660 du 03/07/1985 sur les droits d'auteur et la protection des logiciels.
- Loi n° 91-646 du 10/07/1991 relative au secret des correspondances émises par voie de télécommunication.
- Loi n° 92-597 sur la propriété intellectuelle
- Loi n° 2000-230 du 13/03/2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
- Loi n° 2004-575 du 21/06/2004 pour la confiance dans l'économie numérique.
- Loi n°2012-410 du 27/03/2012 relative à la protection de l'identité.
- Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractères personnel et à la libre circulation de ces données
- Règlement général de sécurité (RGS) décret 2010-112 et ordonnance 2005-1516

14.1. Le Droit Disciplinaire

- Ordonnance n°2021-1574 du 24 novembre 2021 septembre 1989 relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux.
- Loi n°83-634 du 13 juillet 1983, article 28 sur le respect de la hiérarchie et le secret professionnel
- Ordonnance n°2021-1574 du 24 novembre 2021 fixant les dispositions communes applicables aux fonctionnaires stagiaires de la Fonction Publique Territoriale.
- Décret n°88-145 du 15 février 1988 (art. 36 et 37) relatif aux agents contractuels.
- Décret n°91-298 du 20 mars 1991 (art. 15) relatif aux agents à temps non complet.

14.2. Le Code Pénal

Code Pénal Livre 3 Titre 2 Chapitre III : Des atteintes aux systèmes de traitement automatisé de données.

- **Article 323-1 :**

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60.000 euros d'amende.

- **Article 323-2 :**

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150.000 euros d'amende. »

- **Article 323-3 :**

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150.000 euros d'amende. »

- **Article 323-4 :**

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

- **Article 323-5 :**

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

- 1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26.
- 2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.
- 3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution.
- 4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés.
- 5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

- 6º L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés.
- 7º L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35. »

- **Article 323-6 :**

« Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.
Les peines encourues par les personnes morales sont :

- 1º L'amende, suivant les modalités prévues par l'article 131-38.
- 2º Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2º de l'article 131-39.
Porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

- **Article 323-7 :**

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

- **Article 226 :**

  « Le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :
  - 1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
  - 2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé. »

14.3. Le Code Civil

Article 1242 (Ex-article 1384 alinéa 5) relatif aux différentes manières dont on acquiert la propriété

14.4. Contacts utiles

Plateforme GLPI
https://supportglpi.sitiv.fr/
Se connecter avec votre adresse Mail et votre mot de passe habituel

Délégué à la protection des données :
04 77 31 05 92
securite-si@sitiv.fr

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

CHARTE INFORMATIQUE

Table des matières

1. Préambule 3
2. Le champ d'application 4
2.1. Le système d'information et communication 4
2.2 Les utilisateurs 5
2.2.1 – Les visiteurs 6
2.2.2 – Les administrateurs 6
3. Conditions générales d'utilisations 7
3.1 Confidentialité 7
3.1. Sécurité 7
3.2. Utilisation à des fins personnelles 10
3.3. Protection et propriété des données produites par les utilisateurs 12
4. Internet 13
5. Messagerie électronique 14
5.1. Mise à disposition 14
5.2. Règles d'utilisation 14
5.2.1. Utilisation professionnelle 14
5.2.2. Utilisation personnelle 15
5.2.3. Sécurité et filtrage 15
6. Les réseaux sociaux, blogs et forums 17
7. Téléphonie et smartphone fournis par le SITIV 18
8. Droit à la déconnexion 19
9. Photocopieurs et scanners 20
10. Données personnelles 21
11. Contrôle des activités 24
12. Information et sanctions 25
13. Entrée en Vigueur 27
14. Annexes 28
13.1 La Réglementation 28
14.1. Le Droit Disciplinaire 28
14.2. Le Code Pénal 29
14.3. Le Code Civil 31
14.4. Contacts utiles 31

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

1. Préambule

Le SITIV met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des outils mobiles.

Le SITIV s'engage à :

- Mettre à disposition les ressources informatiques matérielles et logicielles nécessaires au bon déroulement de la mission des utilisateurs.
- Mettre en place des programmes de formation adaptés et nécessaires aux utilisateurs pour une bonne utilisation des outils.
- Informer les utilisateurs des diverses contraintes d'exploitation (interruption de service, maintenance, modification de ressources…) du système d'information susceptibles d'occasionner une perturbation.
- Effectuer les mises à jour nécessaires des matériels et des logiciels composant le système d'information afin de maintenir le niveau de sécurité en vigueur dans le respect des règles d'achat et des budgets alloués.
- Respecter la confidentialité des "données utilisateurs" auxquelles il pourrait être amené à accéder pour diagnostiquer ou corriger un problème spécifique.

La vocation de notre charte informatique réside dans l'encadrement de l'utilisation des moyens informatique mis en place par notre service public le « Syndicat Intercommunal des Technologies de l'Information pour les Villes » (SITIV) en tant qu'employeur, enregistré au SIREN 256 910 183 et représenté par son Président.

Ces objectifs se déclinent comme suit :

- Sensibiliser les utilisateurs aux risques et conséquences d'une action volontaire ou involontaire pouvant compromettre le système d'information tels que :
  - Risque de piratage/attaque informatique
  - Utilisation abusive des ressources de l'entreprise
  - Détention et/ou diffusion d'informations et/ou de données protégées par la loi
  - Préjudice à l'image du Syndicat
- Informer les utilisateurs sur les modalités d'utilisation des ressources informatiques.
- Définir les sanctions disciplinaires en cas de manquement à cette même charte.
- Dans le cadre de la loi, informer des contrôles effectués par le syndicat.

2. Le champ d'application

2.1. Le système d'information et communication

La présente charte s'applique au système d'information et de communication du SITIV, notamment constitué d'un ensemble "matériels - système d'exploitation - logiciels" mis à disposition des utilisateurs :

- Matériel informatique et téléphonique :
  - Unités centrales, écrans, claviers, souris, casque etc. qu'ils s'agissent d'ordinateurs (fixes ou portables), périphériques y compris clés USB, disques durs externes…
  - Imprimantes, photocopieurs, scanners, fax
  - Téléphones, smartphones, tablettes et clés 4G
- Système d'exploitation et logiciels :
  - Windows, Linux, macOS, androïd…,
  - Logiciels : pack bureautique, logiciels de gestion, applications spécifiques,
  - Abonnements à des services interactifs,
  - Système de messagerie, réseaux sociaux
- Réseau informatique et infrastructures :
  - Serveurs, routeurs, firewall et connectique,
  - Connexion internet, intranet, extranet, wifi, cloud

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des salariés connecté au réseau du SITIV, ou contenant des informations à caractère professionnel concernant le SITIV.

À défaut de qualification explicite, le patrimoine de données des Villes adhérentes du SITIV, des membres de l'entente TNO et/ou des partenaires auxquels le SITIV et ses utilisateurs/collaborateurs ont accès dans le cadre de l'exercice de leurs activités sont considérées comme interne et sont à ce titre confidentiel.

2.2 Les utilisateurs

Sauf indication contraire, les directives énoncées dans cette charte sont applicables à la totalité des utilisateurs, des données et des systèmes d'informations et de communication du SITIV, à distance ou en présentiel et ceux sans distinction de statut et de temporalité (stagiaires, agents, invités, etc.)

Elle s'applique également à tout partenaire ou prestataire extérieur ayant accès aux données et aux outils informatiques du SITIV.

Chaque utilisateur doit adopter une attitude responsable et respecter les règles définies sur l'utilisation des ressources et notamment :

- Prendre soin des outils de travail fournis par le SITIV et s'engage à les restituer à son départ.
- En cas de perte, de vol ou de détérioration d'une ressource signaler l'incident le plus rapidement possible au service Hébergement/Infrastructure.
- Ne pas masquer son identité, ni usurper l'identité d'autrui, ni prêter son compte. Respecter les règles relatives à l'identification et l'authentification, sachant qu'il est interdit d'utiliser le compte ou s'authentifier en tant qu'un autre utilisateur.
- S'assurer de l'intégrité et la confidentialité des données et ne pas perturber la disponibilité du système d'information.
- Ne pas stocker ou transmettre d'informations portant atteinte à la dignité humaine, ni envoyer ou transférer des messages dont le contenu est irrespectueux, provocant, injurieux, dégradant, malveillant, menaçant, et en règle générale, dont le contenu est contraire aux bonnes mœurs.
- Ne pas marquer les données exploitées d'annotations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et images de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée
- Respecter le droit de propriété intellectuelle : non reproduction et/ou non diffusion de données soumises à un droit de copie non-détenu, interdiction de copie de logiciel sans licence d'utilisation
- Ne pas porter atteinte à la sécurité du système d'information par l'utilisation de "ressources extérieures" matérielles ou logicielles
- Respecter les contraintes liées à la maintenance du système d'information.

- Prendre connaissance et appliquer pour ses usages l'ensemble des prescriptions de la PSSI et de ses annexes.

2.2.1 – Les visiteurs

Les personnes extérieures, de passage dans les locaux et sites du SITIV, pourront bénéficier, pour leurs équipements personnels, d'un accès réseau internet « invités ». Cet accès « invité » sera rendu accessible par le service Infrastructure et Hébergement selon les modalités techniques mise en œuvre par le SITIV.

Une trace du trafic sur ce réseau « invité » pourra être faite dans le but d'identifier d'éventuels incidents de sécurité ou d'exploitation.

Le SITIV ne peut être tenue responsable d'éventuels dommages sur les équipements personnels, lors d'une utilisation « réseau invité ».

2.2.2 – Les administrateurs

Les administrateurs du système d'information et communication veillent au bon fonctionnement du système, à sa disponibilité, sa maintenance, sa sécurité et son évolution pour répondre aux mieux aux besoins du SITIV.

Ils mettent en œuvre toutes les procédures et ressources nécessaires afin d'apporter services et supports aux utilisateurs.

En fonction de leur champ d'activité et de responsabilité, les administrateurs du système d'information et communication, sont soumis au secret professionnel et ne peuvent divulguer des informations à caractère personnel ou privé, auxquelles ils pourraient avoir accès dans le cadre de leur missions et fonctions.

3. Conditions générales d'utilisations

3.1 Confidentialité

Tout utilisateur dispose d'un droit d'accès au système d'information et communication. Ce droit d'accès est unique et personnel.

Les droits d'accès et d'utilisation du système d'information et communication du SITIV sont donnés par les administrateurs. Ces droits sont limités aux activités exercées pour le SITIV et disparaissent lorsque l'utilisateur quitte le syndicat ou que la mission du prestataire prend fin.

Ces droits d'accès peuvent être suspendus, si le comportement d'un utilisateur n'est pas compatible avec les règles énoncées dans la présente charte, ou pour des raisons de sécurité.

Lors de la première utilisation des identifiants (login/mot de passe) l'utilisateur devra modifier son mot de passe qui lui a été communiqué par le service Hébergement & Infrastructure, par un mot de passe personnel, qu'il s'engage à ne pas divulguer et qui devra respecter le degré de complexité défini par le SITIV dans le cadre de sa PSSI.

Pour certaines applications ou supports nécessitant un identifiant et/ou un mot de passe distinct, l'utilisateur devra privilégier l'utilisation du coffre-fort à mots de passe mis à disposition par le SITIV.

L'utilisateur ne doit pas prendre, modifier ou tenter de déchiffrer le mot de passe d'un autre utilisateur.

3.1. Sécurité

Les attaques informatiques ou une mauvaise utilisation de ces outils peuvent avoir des conséquences extrêmement graves.
En effet, ils augmentent les risques d'atteinte à la confidentialité, de mise en jeu de la responsabilité, d'atteinte à l'image, à la réputation, à l'intégrité et à la sécurité des fichiers, des données personnelles (virus, intrusions sur le réseau interne, vols de données).
Les outils informatiques peuvent aussi être une source de perte de productivité et de coûts additionnels.
Le SITIV met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et communication.

A ce titre, les accès aux ressources sensibles sont limités. Le service Hébergement est responsable de la mise en œuvre et du contrôle du bon fonctionnement du système d'information et de communication et 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.
L'utilisateur est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions et missions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence et de vigilance, à savoir :

- En cas d'absence momentanée, même très courte l'utilisateur doit :
  - Verrouiller son PC (Ex. : maintenir enfoncées les touches 'Ctrl+Alt+Suppr' ou « Touche drapeau Windows L » et cliquer sur 'Verrouiller l'ordinateur'), en cas d'oubli un verrouillage automatique se mettra en place.
  - L'utilisateur doit quitter logiciels métiers (déconnexion) et verrouiller son PC.

- A la fin de sa journée de travail, l'utilisateur doit quitter les applications, arrêter le système par arrêt logiciel, le poste de travail et éteindre l'écran.

- Un premier niveau de sécurité consiste à utiliser des mots de passe sûrs non communiqués à des tiers et régulièrement modifiés (une fois par an).

- La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde quotidienne des informations sur les serveurs et non le disque local.

- L'utilisateur doit signaler tous dysfonctionnements ou anomalies à la hiérarchie et au RSI. *(exemple : un tiers non autorisée se rendant compte qu'il a accès à des informations confidentiel via son compte utilisateur)*
- L'utilisateur doit signaler au RSSI toute violation ou tentative de violation suspectée de son compte utilisateur.

- L'utilisateur doit procéder régulièrement à l'élimination des fichiers non- utilisés et à l'archivage, dans le but de préserver la capacité de mémoire, et selon les règles d'archivage légal.

- L'usage des supports amovibles (CD, clé USB, etc.) est interdit.

- L'utilisateur ne doit pas supprimer ou désactiver ou chercher à contourner les mesures de sécurité (antivirus, firewall et autres) installées sur les équipements locaux, distants ou sur toute partie du système d'information et communication du SITIV.

- L'utilisateur doit être particulièrement vigilant lors de l'envoi d'informations sensibles sur les moyens de communication non sécurisés : SMS, messagerie électronique ou Internet.

- Dans le cadre de ses activités professionnelles, l'utilisateur ne doit utiliser que les matériels mis à disposition par le SITIV pour se connecter au système d'information.

- L'utilisateur s'interdit toute installation de logiciel non nécessaire à l'exécution de ses missions et/ou non validé par la collectivité.

La signature électronique (loi n° 2000-230 du 13 mars 2000) est présumée fiable jusqu'à preuve du contraire. Son utilisation est limitée aux personnes autorisées et doit respecter la procédure définie par le SITIV.

3.2. Utilisation à des fins personnelles

L'utilisation des équipements informatiques (matériels et logiciels), numériques et téléphoniques du SITIV est limitée à un usage professionnel.

Durant les heures de travail, il est toléré un usage modéré et très occasionnel, à condition que cela n'entrave pas l'activité professionnelle (la sienne et celle de ses collègues) de :

- L'accès à Internet pour des besoins personnels
- Un usage ponctuel du téléphone pour des communications personnelles locales (une attention particulière est demandée en cas d'appel sur des numéros surtaxés). Le SITIV peut procéder au contrôle de l'ensemble des appels émis.

En dehors des heures de travail, cette utilisation à titre privé est acceptée, sous réserve qu'elle ne perturbe pas l'activité professionnelle du service, ni ne porte atteinte à l'image du SITIV.

Le SITIV se réserve le droit de restreindre ou suspendre temporairement cette utilisation privée, sans préavis en cas de danger pour le système d'information.
Tout utilisateur ayant une utilisation abusive des moyens informatiques (accès à des sites web non professionnels, impression de documents personnels, minage de cryptomonnaie, p2p…), numériques ou téléphoniques sera averti, puis éventuellement sanctionné.
Le SITIV se réserve ainsi la possibilité d'avoir des relevés d'usages de son système d'information et communication. Si une anomalie est constatée, un relevé détaillé des consommations du poste pourra être demandé ainsi que des explications auprès du titulaire du poste.

Les données personnelles de l'utilisateur, qu'il s'agisse de fichiers ou d'autres types de données, doivent être clairement identifiées en utilisant les termes « Privé » ou « Perso » ou « Personnel » dans leurs noms et/ou celui du répertoire les stockant, et/ou dans le nom du disque réseau, qui devra être désigné comme « P:\».

Afin d'éviter toute confusion, il ne faut en aucun cas mettre la mention « CONFIDENTIEL »

Les messages envoyés doivent être signalés également par la mention « Privé » ou « Personnel » dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé « Privé » ou « Personnel ».
Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé « Privé » ou « Personnel ».

En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Les données, fichiers et messages électroniques expressément désignés comme personnels ou privés par un utilisateur ne seront accessibles par le SITIV qu'en présence de l'utilisateur ou en cas de risques majeurs portant atteinte au système d'information et communication.

En cas de manquement de désignation du caractère personnel ou privé des messages, ceux-ci sont présumés être à caractère professionnel.

En cas de départ d'un utilisateur, l'ensemble des données personnelles ou privées qu'il laisserait dans le système d'information et communication du SITIV serait détruit dans un délai maximum d'un mois après son départ.

Par ailleurs, l'utilisateur ne doit pas effectuer de copie de logiciel. En effet, l'utilisation et la diffusion de logiciels acquis illégalement et en irrespect du Code de la Propriété Intellectuelle (loi 92-597) constituent un délit de contrefaçon passible d'amende et d'emprisonnement.

3.3. Protection et propriété des données produites par les utilisateurs

Au SITIV, le travail sur le réseau constitue une règle qui s'impose à tous.
En effet, seuls les fichiers enregistrés sur le réseau font l'objet d'une sauvegarde générale et quotidienne.
Travailler sur le réseau constitue donc, pour tous, un impératif de sécurité et de conservation des données.
Les archives de chaque utilisateur constituent la mémoire du SITIV et garantissent la continuité d'activité. Cela signifie en particulier :

- Que les collaborateurs ne travaillent pas en individualité mais pour le compte du SITIV qui les emploie. Ils ne sont donc pas « propriétaire » de leur travail. Leurs documents et fichiers informatiques doivent être correctement nommés, de manière normative, voire datée, classés en arborescence par dossiers et sous dossiers, de manière thématique et non personnalisée et organisés comme doivent l'être les dossiers physiques ;
- Le travail en local sur disque « C » est à éviter, car il ne fait pas l'objet d'une sauvegarde.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

4. Internet

Dans le cadre de leur activité, les Utilisateurs ont accès à internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé.

L'utilisateur s'engage lors de ses consultations Internet à ne pas se rendre sur des sites portant sur des sujets pénalement répréhensibles (pédopornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée…).

Le téléchargement, en tout ou partie, de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux ou films, logiciels propriétaires, etc.) est strictement interdit.

De même, le visionnage de films et l'écoute de musique en streaming, non liés à l'activité professionnelle ne sont pas autorisés.

Le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet est interdit.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

5. Messagerie électronique

5.1. Mise à disposition

Le SITIV met à disposition aux utilisateurs des adresses électroniques, la majorité, sauf cas particuliers[1], suivent la politique de nommage suivante : 1ère lettre du prénom de l'utilisateur, suivi du son nom@sitiv.fr.

(¹ pour exemple : adresse de contact utile tel que securite-si@sitiv.fr, impossibilité d'appliquer la politique de nommage car adresse déjà existante, etc.)

L'utilisation de la messagerie est principalement réservée à des fins professionnelles. Dans ce cadre, cette messagerie est donc susceptible d'être ouverte par les administrateurs afin de garantir une sécurité du système, une continuité de service… Cette démarche ne sera mise en œuvre qu'après validation de la direction générale, suite à la demande du responsable de service ou avec l'accord formel de l'utilisateur.

Pour le partage de fichiers, l'utilisateur privilégiera la plateforme collaborative ou serveur partagé, mis à disposition par le SITIV (type cloud).

5.2. Règles d'utilisation

5.2.1. Utilisation professionnelle

L'utilisateur s'engage à ne pas envoyer en dehors des services du SITIV des informations professionnelles nominatives ou confidentielles, sauf si cet envoi est à caractère professionnel et autorisé par son supérieur hiérarchique.

L'utilisateur soigne la qualité des informations envoyées à l'extérieur et s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine, à la vie privée, aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.

L'utilisateur signera tout courriel professionnel.

Il doit vérifier la liste des destinataires. Il doit également vérifier le contenu et l'historique des messages transférés (gestion du "Répondre à tous").

L'utilisateur doit éviter de surcharger le réseau d'informations inutiles, par exemple en évitant de mettre automatiquement des accusés de réception et de lecture de mails. Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier « éléments supprimés » doit être vidé périodiquement.

En cas d'absence prévisible, l'utilisateur devra mettre en place un message automatique d'absence indiquant la date de retour prévue et invitant le correspondant à rediriger son mail vers un agent ou l'adresse générique du service qui pourra gérer les messages et demandes pendant son absence.

En cas d'absence non prévisible, l'administrateur pourra, si nécessaire, ajouter un message d'absence réorientant vers une autre adresse mail et de préférence une adresse mail générique.

5.2.2. Utilisation personnelle

Les courriers à caractère privé et personnel doivent expressément porter la mention « personnel » ou « privé » ou « perso » dans leur objet ou être classés dans un dossier spécifique « personnel » ou « privé » ou « perso ».

Afin d'éviter toute confusion, il ne faut en aucun cas mettre la mention « CONFIDENTIEL » en objet d'un message personnel, le terme « confidentiel » pouvant être utilisé dans le domaine professionnel.

En cas de manquement à ces règles, les courriers sont présumés être à caractère professionnel.

Pour réduire le risque d'utilisation abusive, l'adresse e-mail étant attribué à l'utilisateur ne doit pas être utilisée pour s'identifier ou s'inscrire sur des forums, réseaux sociaux, messageries instantanées, sites d'achats et autres sites sans rapport avec l'activité professionnelle.

5.2.3. Sécurité et filtrage

L'utilisateur doit veiller à ne pas ouvrir les courriels dont le sujet paraîtrait suspect. Ces messages peuvent contenir des programmes malveillants dont potentiellement des systèmes de cryptage de fichiers, appelé cryptoLocker et/ou ransomwares qui est en fait un logiciel malveillant pouvant se propager.

Enfin, un mécanisme de filtrage des mails entrants a été mis en place permettant ainsi de supprimer les mails non sollicités (SPAM) et/ou représentant des menaces pour le système d'information et communication du SITIV.

Les filtres d'entrée des courriers indésirables permettent d'économiser les ressources informatiques du SITIV tant en termes de réseau que de stockage, et de protéger les utilisateurs contre certains types de menaces.

Les utilisateurs ont la possibilité de consulter la liste des mails envoyés à leur adresse et rejetés par le système. Ils peuvent constituer leurs propres listes blanches et listes noires d'expéditeurs à autoriser ou interdire expressément.

Les mails sortants sont également analysés par un antivirus pour éviter la propagation.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

6. Les réseaux sociaux, blogs et forums

L'utilisation des réseaux sociaux est réservée à des fins professionnelles.

De manière générale, toute publication d'information interne, financière, stratégique et/ou confidentielle du SITIV sur les réseaux sociaux, blogs ou forums est interdite.

Des autorisations de communication sur les réseaux sociaux, blogs ou forums sont attribuées aux collaborateurs, aux services, qui sont habilités à parler au nom du SITIV. La distinction entre l'utilisation professionnelle et l'utilisation personnelle est imposée (création de deux profils).

Les utilisateurs doivent veiller au respect des lois et règlements en vigueur et par conséquent, ils ne doivent pas faire de commentaires injurieux, diffamatoires ou racistes, et respecter les lois relatives à la propriété intellectuelle et notamment le droit d'auteur et le droit à l'image.

Les utilisateurs sont personnellement responsables des contenus ou commentaires publiés sur les réseaux sociaux, blogs et forums.

Par ailleurs, il est rappelé, au titre des droits et obligations des fonctionnaires (discrétion professionnelle, devoir de réserve et devoir de neutralité), que la liberté d'expression sur les réseaux sociaux, blogs et forums n'est pas sans limite pour l'utilisateur (agent titulaire ou contractuel). L'utilisateur doit respecter les obligations déontologiques, même en dehors du service.

En effet, lorsqu'il s'exprime publiquement sur les réseaux sociaux, blogs ou forums soit à titre personnel soit au titre d'autre qualité comme celle d'une association, l'utilisateur ne doit pas faire état de sa qualité au sein de l'établissement.

L'utilisateur doit ainsi éviter toute manifestation d'opinion de nature à porter atteinte à l'image du SITIV. Enfin, l'utilisateur s'engage à ne pas alimenter de polémique et/ou écrire des textes contraires à la bien séance et/ou à la loi dans un site de type « réseau social » (Facebook, Twitter, LinkedIn etc…) un site type « blogs » ou « forum » avec son adresse mail professionnelle, ni de poster des vidéos, des fichiers, des programmes contraires à la bien séance et/ou à la loi.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

7. Téléphonie et smartphone fournis par le SITIV

L'utilisation des téléphones fixes et portables fournis par le SITIV est réservée à des fins professionnelles.

Le smartphone est un outil de travail dont l'usage personnel peut être autorisé (mention "personnel" pour messages personnels)

Il n'est pas attendu de répondre aux appels ou aux mails en dehors du temps de travail (soir, week-end et congé.)

Il est rappelé que l'usage de téléphone portable n'est pas autorisé en conduisant, sauf véhicule équipé en Bluetooth et ceci de manière très occasionnelle.

En cas d'absence, l'utilisateur doit effectuer un renvoi sur le poste d'un autre agent du service ou sur l'accueil téléphonique. L'agent qui quitte définitivement le SITIV doit restituer le téléphone portable professionnel.

L'utilisation des téléphones portables personnels doit rester limitée, occasionnelle et discrète (appels et sms). Il ne doit pas venir perturber une réunion ou un entretien.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

8. Droit à la déconnexion

L'utilisation des Technologies de l'Information et de la Communication mis à disposition des salariés, doit respecter leur vie personnelle. A cet égard, ils bénéficient d'un droit à déconnexion les soirs, les weekends et pendant leurs congés, ainsi que l'ensemble des périodes de suspension de leur contrat de travail, sauf circonstances exceptionnelles.

Ce droit à la déconnexion consiste à éteindre et/ou désactiver les outils de communication mis à leur disposition comme le téléphone portable, l'ordinateur portable et la messagerie électronique professionnelle en dehors des heures habituelles de travail. Les salariés pourront même durant leurs temps de repos laisser ces outils au sein de la société en ayant informé parallèlement leur supérieur hiérarchique.

L'entreprise précise que les salariés n'ont pas l'obligation, hors plages de travail habituelles, en particulier, en soirée, les week-ends et lors de leurs congés, de répondre aux courriels et appels téléphoniques qui leur sont adressés. Il leur est demandé également, pendant ces périodes, de limiter au strict nécessaire et à l'exceptionnel l'envoi de courriels ou les appels téléphoniques.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

9. Photocopieurs et scanners

L'utilisateur s'oblige à respecter des règles d'économie et de non-gaspillage concernant l'usage des imprimantes et des photocopieurs. Ainsi, à l'ère de la dématérialisation, il est recommandé de n'imprimer que les documents qui le nécessitent, de préférer le recto verso et l'impression couleur doit rester une exception.

L'utilisateur est invité à aller récupérer ses impressions et utiliser des copieurs à code d'accès pour les impressions de documents sensibles comprenant des informations confidentielles. L'utilisateur veillera donc à ne pas oublier des documents papiers en attente dans les copieurs en accès libre ou public.

Concernant la numérisation de document, il est conseillé de scanner au format PDF compact et d'enregistrer directement le dossier scanné sur le serveur, ce qui pourra permettre de partager des fichiers via un cloud.

L'utilisation des moyens de reprographie à des fins personnelles est strictement interdit.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

10. Données personnelles

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, complétée et renforcée par le règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractères personnel et à la libre circulation de ces données (RGPD) définit les conditions dans lesquelles des traitements de données personnels peuvent être opérés.
Elle institue au profit des personnes concernées par les traitements des droits que la présente charte informatique invite à respecter, tant à l'égard des utilisateurs que des tiers.

Des traitements de données automatisés et manuels sont effectués dans le cadre des systèmes de contrôle, prévus dans la présente charte. Ils sont, en tant que de besoin, déclarés conformes.

Tout utilisateur pourra avoir accès aux données le concernant et ces données ne seront conservées que sur une période maximale définie au regard de la finalité du traitement, de la licéité du traitement...

Il est rappelé aux utilisateurs que les traitements de données à caractère personnel doivent être conforme au RGPD.
Les utilisateurs souhaitant réaliser, dans le cadre professionnel, des traitements relevant dudit règlement sont invités à prendre contact avec la déléguée à la protection des données à l'adresse securite-si@sitiv.fr.

En effet, toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclaré auprès du Délégué à la Protection des données personnelles du SITIV, qui étudie :

- La pertinence des données recueillies.
- La finalité du traitement.
- Les durées de conservation prévues.
- Les destinataires des données.
- Le moyen d'information des personnes fichées et les mesures de sécurité à déployer pour sécuriser les données.

Tout utilisateur est tenu d'assurer la protection des données à caractère personnel qu'il traite dans le cadre de ses fonctions notamment en :

- Protégeant les codes d'accès aux applications et systèmes d'information qu'il utilise,

- En limitant strictement aux besoins de son activité la diffusion par des moyens informatiques ou autre (impressions papier par exemple) des données à caractère personnel en sa possession,
- En ne conservant pas ces données au-delà de la durée nécessaire au traitement auquel elles sont destinées.

L'utilisateur s'engage à :

- Ne pas utiliser les données à des fins autres que celles prévues par ses attributions ;

- Ne divulguer ces données qu'aux personnes dûment autorisées, qu'il s'agisse de personnes privées, publiques, physiques ou morales ; Les données à caractère personnel relevant de la vie privée des personnes et, collectées par un utilisateur, ne peuvent être communiquées à des tiers et ne seront donc pas publiable, sont notamment concernées les données au titre de : l'état civil, la situation patrimoniale et financière, la domiciliation bancaire la qualité de travailleur handicapé, la formation initiale, les horaires de travail, les sympathies politique et l'appartenance à un parti politique, les croyances religieuses. A l'inverse d'autres données ne sont couvertes par le secret de la vie privée, notamment les données dont on estime que les usagers doivent avoir connaissance, soit au titre de l'organisation du service public, soit afin de pouvoir exercer pleinement un droit de recours (bénéficiaire d'une autorisation d'urbanisme, informations librement consignées sur des registres d'enquête publique…).

- S'assurer que seuls des moyens de communications sécurisés seront utilisés pour transférer ces données ;

- 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 pour préserver la sécurité physique et logique de ces données.

- Prévoir des mesures techniques et organisationnelles pour protéger les données (destruction, perte, altération, diffusion ou accès non autorisés, etc.). Ces mesures doivent assurer un niveau de sécurité approprié aux risques et à la nature des données considérées.

Concernant les archives courantes et intermédiaires, elles relèvent du régime de droit commun du RGPD et de la loi Informatique et liberté, c'est à dire le droit à l'effacement, modification, opposition, portabilité…. Ces droits sont toutefois limités dans certains cas, comme par exemple le droit à l'effacement qui ne s'applique pas lorsqu'il s'agit de respecter une obligation légale ou pour exécuter une mission d'intérêt public.

Concernant les archives définitives, le RGPD et l'article 36 de la loi Informatique et libertés confirment la possibilité de conserver les données au-delà de la durée de conservation prévue dans le traitement initiale, à des fins archivistiques dans l'intérêt publics, à des fins de recherches scientifique ou historique ou statistiques.
Lorsqu'il sera question de supprimer des données à caractère personnel, l'utilisateur est invité à prendre attache auprès du Délégué à la Protection des Données du SITIV.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

11. Contrôle des activités

Les administrateurs du système d'information et communication du SITIV sont amenés à prendre toutes dispositions nécessaires pour assurer le bon fonctionnement des réseaux et moyens informatiques du SITIV et le respect de la présente charte informatique. Des contrôles techniques peuvent ainsi être opérés :

- Dans un souci de sécurité du réseau et/ou des ressources informatiques, de maintenance et de gestion techniques, de respect de la législation applicable et notamment de respect des règles relatives à la protection de la vie privée ;

- Dans un souci de vérification de l'utilisation des moyens informatiques et des télécommunications afin qu'elles restent conformes aux règles édictées par la présente charte.

- Dans un souci de recherche de preuves dans le cadre d'une action judiciaire et/ou d'une atteinte au RGPD, en déclenchant une investigation numérique. Les administrateurs du système d'information et communication disposent d'outils permettant d'analyser tout ce qui transite par celui-ci et grâce aux logs des systèmes peuvent connaître les actions réalisées (sachant que cette liste n'est pas exhaustive) :

- Les connexions au réseau (identifiants, dates et heures de connexion…),

- Les fichiers stockés sur les serveurs (format, date création ou de dernière modification, taille…)

- Les connexions passant par Internet (identifiants de connexion, sites visités, volumes de données transférées, dates et heures de connexion…).

Ces logs sont enregistrés durant une année pour permettre la détection de comportements malveillants ou contraires aux politiques de sécurité du SITIV, de dysfonctionnements du système d'information, l'analyse a posteriori d'incidents de sécurité, pour se conformer aux textes et règlements en vigueur, ainsi que pour contrôler le respect de la présente charte.

Elles peuvent être communiquées aux autorités publiques compétentes en cas de réquisition judiciaire, aux conseils juridiques et également aux services de ressources humaines du SITIV.
Les administrateurs du système d'information et communication sont équipés d'outils permettant une prise en main à distance des postes, des logiciels… Cette prise en main ne s'effectue qu'en présence de l'utilisateur en poste ou avec son accord.
Le contenu même des échanges réalisés par les utilisateurs n'est pas conservé.

12. Information et sanctions

La présente charte est annexée au règlement intérieur. A compté du 12/04/2024, soit l'entrée en vigueur de la présente charte, chaque utilisateur du SITIV s'en verra remettre un exemplaire, il devra en prendre connaissance et devra s'engager à la respecter. Chaque agent sera tenu informé des adaptations via les voies de communication internes.

Les collaborateurs du service hébergement sont à la disposition des utilisateurs pour leur fournir toute information concernant l'utilisation du système d'information et communication, en particulier sur les procédures de sauvegarde et de filtrage.

Elle les informe régulièrement sur l'évolution des limites techniques du système d'information et de communication 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 hébergement dans le cadre de la présente charte.

L'utilisateur ne doit à aucun moment oublier qu'il vit et travaille au sein d'une collectivité. Il s'interdit toute utilisation abusive d'une ressource commune.

Il s'interdit également de perturber tout autre utilisateur du système d'information et communication à l'aide d'outils électroniques, de masquer son identité ou de s'approprier le mot de passe d'un autre utilisateur.

Il s'interdit également de porter atteinte à l'intégrité d'un autre utilisateur, notamment par l'intermédiaire de messages et d'images provocantes. Il s'interdit enfin de saturer la messagerie des autres utilisateurs par l'envoi de messages, trop nombreux ou trop volumineux, non liés à l'activité professionnelle.

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 avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Dans ce dernier cas, les procédures prévues dans le cadre des statuts de la fonction publique seront appliquées. L'utilisation reconnue à des fins personnelles de certains services payants à travers le système de communication donnera également lieu à remboursement de la part de l'utilisateur concerné.

Le SITIV 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 ou de violation du secret des correspondances.
Le manquement à la présente charte pourrait entraîner le retrait du droit d'utilisation d'un outil, d'une application ou d'un matériel informatique/téléphonique et/ou des mesures d'ordre disciplinaire et/ou des sanctions pénales.

Le niveau de sanction sera proportionnel à la faute commise et sera apprécié au regard du manquement aux obligations professionnelles et de la présente charte.

13. Entrée en Vigueur

La présente charte est applicable à compter du 12 Avril 2024.

14. Annexes

L'agent doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par l'ordonnance n°2021-1574 du 24 novembre 2021 portant droits et obligations des fonctionnaires et l'ordonnance n°2021-1574 du 24 novembre 2021 relative à la fonction publique territoriale.

13.1 La Réglementation

- Loi n° 78-17 du 06/01/1978 sur l'informatique, les fichiers, les libertés.
- Loi n° 78-753 du 17/07/1978 sur la liberté d'accès aux documents administratifs.
- Loi n° 85-660 du 03/07/1985 sur les droits d'auteur et la protection des logiciels.
- Loi n° 91-646 du 10/07/1991 relative au secret des correspondances émises par voie de télécommunication.
- Loi n° 92-597 sur la propriété intellectuelle
- Loi n° 2000-230 du 13/03/2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
- Loi n° 2004-575 du 21/06/2004 pour la confiance dans l'économie numérique.
- Loi n°2012-410 du 27/03/2012 relative à la protection de l'identité.
- Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractères personnel et à la libre circulation de ces données
- Règlement général de sécurité (RGS) décret 2010-112 et ordonnance 2005-1516

14.1. Le Droit Disciplinaire

- Ordonnance n°2021-1574 du 24 novembre 2021 septembre 1989 relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux.
- Loi n°83-634 du 13 juillet 1983, article 28 sur le respect de la hiérarchie et le secret professionnel
- Ordonnance n°2021-1574 du 24 novembre 2021 fixant les dispositions communes applicables aux fonctionnaires stagiaires de la Fonction Publique Territoriale.
- Décret n°88-145 du 15 février 1988 (art. 36 et 37) relatif aux agents contractuels.
- Décret n°91-298 du 20 mars 1991 (art. 15) relatif aux agents à temps non complet.

14.2. Le Code Pénal

Code Pénal Livre 3 Titre 2 Chapitre III : Des atteintes aux systèmes de traitement automatisé de données.

- **Article 323-1 :**

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60.000 euros d'amende.

- **Article 323-2 :**

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150.000 euros d'amende. »

- **Article 323-3 :**

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150.000 euros d'amende. »

- **Article 323-4 :**

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

- **Article 323-5 :**

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

- 1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26.
- 2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.
- 3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution.
- 4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés.
- 5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics.

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE

- 6º L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés.
- 7º L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35. »

- **Article 323-6 :**

« Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.
Les peines encourues par les personnes morales sont :

- 1º L'amende, suivant les modalités prévues par l'article 131-38.
- 2º Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2º de l'article 131-39.
Porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

- **Article 323-7 :**

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

- **Article 226 :**

  « Le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :
  - 1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
  - 2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé. »

14.3. Le Code Civil

Article 1242 (Ex-article 1384 alinéa 5) relatif aux différentes manières dont on acquiert la propriété

14.4. Contacts utiles

Plateforme GLPI
https://supportglpi.sitiv.fr/
Se connecter avec votre adresse Mail et votre mot de passe habituel

Délégué à la protection des données :
04 77 31 05 92
securite-si@sitiv.fr

Envoyé en préfecture le 13/04/2024
Reçu en préfecture le 13/04/2024
Publié le
ID : 069-256910183-20240412-CS_2024_04_5-DE