Accusé de réception en préfecture
041-214102691-20230920-VVSG20230920-16-AR
Date de télétransmission : 29/09/2023
Date de réception préfecture : 29/09/2023
Date de publication le 29 septembre 2023

- COMMUNE DE VENDÔME -
(Loir-et-Cher)

ARRÊTÉ

Arrêté n° VVSG20230920-16

OBJET : ADMINISTRATION GENERALE - Charte informatique

Le Maire ;
Vu le code général des collectivités territoriales et notamment l'article L. 2122-18 qui dispose que le maire est seul chargé de l'administration ;
Vu le procès-verbal d'élection du conseil municipal de Vendôme du 28 mai 2020 proclamant Laurent Brillard maire de Vendôme ;
Vu la charte sur le bon usage de l'outil informatique et de la messagerie en vigueur depuis le 1er septembre 2008 ;
Considérant qu'en tant que chef de l'administration communale, le maire est le supérieur hiérarchique des agents de la commune et dispose d'un pouvoir d'organisation des services ;
Considérant alors qu'il prend les mesures relatives à l'organisation interne des services et la gestion interne de ses agents ;
Considérant que le développement du système d'information nécessite l'évolution et l'adaptation des méthodes de travail et exige une sécurisation de son emploi ;
Considérant qu'il est donc nécessaire de règlementer l'utilisation du système d'information ;
Considérant que la charte en vigueur depuis 2008 nécessite d'être profondément modifiée en raison de l'évolution du système d'information et de l'usage de celui-ci ;
Vu l'avis favorable du comité social territorial du 19 septembre 2023.

ARRÊTE

ARTICLE 1 : La charte sur le bon usage de l'outil informatique et de la messagerie en vigueur depuis le 1er septembre 2008 est abrogée au 1er octobre 2023.

ARTICLE 2 : La charte informatique telle qu'annexée vient réglementer les modalités d'accès et d'utilisation du système d'infomation de la collectivité par les agents de la Ville de Vendôme ; elle explicite les droits et les devoirs des utilisateurs et de l'administrateur.

ARTICLE 3 : La charte entre en vigueur au 1er octobre 2023.

ARTICLE 4 : La charte a une valeur normative et sa violation peut entraîner des sanctions.

ARTICLE 5 : La charte sera annexée au règlement intérieur.

ARTICLE 6 : Le présent arrêté sera transmis au représentant de l'État dans le département et publié. Il sera affiché, publié et inscrit au registre des arrêtés.

ARTICLE 7 : Dans un délai de deux mois à compter de la date de publication du présent arrêté, les recours suivants peuvent être introduits en recommandé avec accusé de réception :

- un recours gracieux adressé au maire de Vendôme, BP 20107, 41106 Vendôme cedex. Au terme d'un délai de deux mois, le silence du maire vaut rejet implicite du recours gracieux ;
- un recours contentieux auprès du tribunal administratif d'Orléans, 28 rue de la Bretonnerie, 45000 Orléans. Le tribunal administratif peut être saisi par l'application informatique Télérecours citoyens accessible par le site internet http://www.telerecours.fr.

Fait à Vendôme, le 20 septembre 2023

POUR EXTRAIT CONFORME
Le Maire
Laurent BRILLARD

PJ : Charte informatique

Charte Informatique

Préambule

L'objet de cette charte est de décrire les engagements des agents, accédant au système d'informations. Cette charte vise à informer, sensibiliser et responsabiliser tous les acteurs de la collectivité et fixe les principes, les modalités d'accès et d'utilisation des outils informatiques de la collectivité.

Cette charte s'applique à l'ensemble des agents de l'administration territoriale : la Communauté d'agglomération Territoire vendômois, la ville de Vendôme, le Centre intercommunal d'action sociale de Territoires vendômois (CIAS), le Centre communal d'action sociale de Vendôme (CCAS) et la Régie du Pôle nautique de Territoires vendômois (RPN).

Cette charte informatique s'inscrit dans la mise en œuvre de la politique de sécurité des systèmes d'information.

Les principes énoncés ne sont pas exclusifs de l'application des lois, du règlement intérieur de la collectivité, des devoirs incombant aux agents, et des règles minimales de courtoisie et de respect d'autrui.

Nous demanderons à chaque agent utilisant les outils mis à disposition de la collectivité d'avoir pris connaissance de cette charte. Elle sera annexée au règlement intérieur.

La présente charte entre en vigueur le 1er octobre 2023.

Table des matières

Modalités d'intervention des équipes chargées de la gestion des ressources informatiques de la collectivité

Article 1 – Engagement de confidentialité de la Direction des systèmes d'information et des télécommunications (DSIT)

Comme tous les agents de nos collectivités, l'ensemble de l'équipe de la DSIT est soumise à l'obligation de discrétion professionnelle telle que prévue par l'article 121-7 du code général de la fonction publique.
Comme pour tous les agents de nos collectivités, le respect de cette obligation implique le respect de la confidentialité des données dont ils ont connaissance dans le cade de leur mission.

Article 2 – Contrôle des accès et usages des ressources par la DSIT

Dans le respect des principes de transparence et de proportionnalité, à des fins de sécurité et de vérification du bon accès et usage des ressources ainsi que du fonctionnement des systèmes d'informations, la collectivité a mis en place des procédures pour superviser l'usage des ressources informatiques et assurer le bon fonctionnement des systèmes de filtrage et de contrôle (pare-feu, systèmes de contrôle des accès, anti-malware, journaux de logs, etc.).
L'agent est informé que :

- pour effectuer la maintenance corrective, curative ou évolutive, la collectivité se réserve la possibilité de réaliser des interventions sur les ressources matérielles et logicielles mises à sa disposition, ou de réaliser une prise de main à distance. Cette dernière est précédée d'une information de l'utilisateur et **doit être acceptée par ce dernier** ;
- toute situation bloquante pour le système, générant une difficulté technique ou une faille de sécurité, pourra conduire à l'isolement du poste voir à la suppression des données en cause ;
- l'utilisation de l'ensemble du système d'information peut donner lieu à un contrôle à des fins statistiques, de traçabilité réglementaire, de suivi fonctionnel, de suivi de consommation, d'optimisation d'usage des licences, de sécurité ou de détection des abus, dans le respect de la législation applicable ;
- l'utilisation qu'il fait des ressources est susceptible d'être contrôlée a posteriori.

Article 3 – Sauvegarde

Vos données sont à enregistrer de préférence sur le réseau bureautique.

- un répertoire existe pour chaque service : (S:) ;
- un répertoire personnel est mis à disposition des agents : (P:) ;
- un espace commun existe également : (Q:).

Il est déconseillé de stocker vos documents sur votre disque dur d'ordinateur :

- celui-ci n'est pas sauvegardé ;
- en cas de perte ou de vol, les données sont perdues ;
- allonge le temps de traitement du remplacement des postes pour la DSIT.

Les données stockées sur le serveur bureautique sont sauvegardées quotidiennement puis conservées un mois. Les sauvegardes hebdomadaires et mensuelles sont conservées un an.
Ceci implique, entre autres, que la suppression par un utilisateur d'un fichier sur le serveur bureautique n'est pas absolue et qu'il en reste une copie :

- sur le dispositif de sauvegarde ou miroir ;
- sur la cassette de sauvegarde.

En cas de suppression par erreur, merci de bien vouloir indiquer le chemin d'accès du document à restaurer dans une demande GLPI.

Moyens d'authentification utilisés par la collectivité

Article 4 – Habilitations et mots de passe

Le contrôle d'accès logique, identifiant + mot de passe, permet d'identifier toute personne utilisant un ordinateur.
Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.
Même si les droits confiés sont plus larges que le nécessiterait votre fonction, vous ne devez utiliser les applications et accéder aux informations que pour les stricts besoins de votre fonction et de vos attributions.
Une identification (login + mot de passe) unique est confiée à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite.

Article 5 – Définition du mot de passe

Un mot de passe doit, pour être efficace, comporter 12 caractères. Il ne doit pas être, notamment, identique au login même en inversant les caractères, compter le nom et/ou prénom de l'utilisateur ou son numéro de téléphone. Les 12 caractères doivent contenir au minimum ; une majuscule, une minuscule, un chiffre et un caractère spécial.
Chaque mot de passe doit obligatoirement être modifié selon la fréquence suivante : 6 mois.

Article 6 – Règle de sécurité du mot de passe

La DSIT se réserve le droit d'imposer un changement de mot de passe à des utilisateurs pour des raisons de sécurité.
Un agent ne doit en aucun cas communiquer son identifiant / mot de passe à un tiers.
L'agent devra signaler à la DSIT toute violation ou tentative de violation suspectée de son compte informatique.

Confidentialité

Article 7 – Cadre Juridique

Tout agent s'engage, conformément aux articles 121 et 122 de la loi du 6 janvier 1978 modifiée au 1er juin 2019 relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 28 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin de protéger la confidentialité des informations auxquelles il a accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Article 8 – Engagement pour la protection des données

Dans le cadre de réglementation sur la protection des données personnelles (RGPD), il revient aux agents responsables de traitements ou créateurs de fichiers contenant des données personnelles d'en faire la déclaration auprès du délégué à la protection des données (DPO) de la collectivité avant toute utilisation.
L'agent s'engage à :

- ne pas accéder, tenter d'accéder ou supprimer des informations si cela ne relève pas des tâches incombant à l'agent ;
- ne pas utiliser les données auxquelles il / elle peut accéder à des fins autres que celles prévues par ses attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de ses missions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes à l'usage et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- s'assurer, dans la limite de ses attributions, que seuls des moyens de communication sécurisés validés seront utilisés pour transférer ces données ;
- faire preuve de discrétion professionnelle ; se rapporter à l'article 26 de la loi n° 83.634 du 13 juillet 1983 ;
- verrouiller son ordinateur dès qu'il quitte son poste de travail ;
- prévenir immédiatement la DSIT dès connaissance de la perte ou vol d'un équipement informatique.

Modalités d'utilisation des moyens informatiques et de télécommunications

Article 9 – Utilisation du poste de travail

Il est interdit d'installer quelconque logiciel sur votre ordinateur ou de connecter un dispositif personnel dessus. Seul la DSIT est autorisée à installer des applicatifs sur votre poste de travail.
En cas de besoin d'équipements particuliers en lien avec la santé, merci de vous rapprocher de la préventrice qui nous transmettra la demande.

Article 10 – Utilisation des équipements de prêt

Pour des raisons de sécurité, le login "vendome" sans mot de passe n'est plus disponible sur les ordinateurs portables de prêt.
Vous devrez donc, comme dans la salle de réunion de l'aile Saint-Jacques, vous connecter avec vos identifiants.

De même vous devrez vous connecter, à votre session, une première fois au réseau, que ce soit en filaire ou sur le Wifi DSIT, avant d'emmener l'ordinateur de prêt.

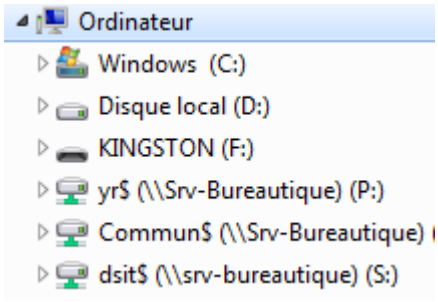
Article 11 – Utilisation des supports amovibles

L'utilisation de clés USB avec des données sensibles et confidentielles de la collectivité est fortement déconseillée.
Pour des raisons de sécurité, avant toute utilisation d'une clé USB, ayant été connecté à un ordinateur autre qu'appartenant à la collectivité, sur votre ordinateur, il est obligatoire de procéder à une analyse antivirus en dehors du réseau de la collectivité.

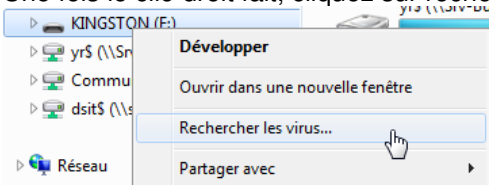
Merci de suivre la procédure ci-dessous :

- Se déconnecter du réseau :
    - Filaire (Débrancher le câble réseau) ;
    - Wifi et/ou 4G ;
    - VPN.
- Brancher la clé USB et réaliser l'analyse antivirus.

Aller dans votre explorateur Windows.
Faites un clic-droit sur la clé USB comme suit (en l'occurrence KINGSTON (F)) :



Une fois le clic-droit fait, cliquez sur rechercher les virus comme suit :



Cette action lancera l'analyse. Vous ne devez utiliser la clé que si vous obtenez un résultat positif, c'est-à-dire sans risque.
Dans le cas contraire, merci de contacter immédiatement le service informatique et de ne pas rebrancher votre ordinateur au réseau.
Merci de prendre note que l'antivirus est susceptible de supprimer automatiquement et sans consentement des données de la clé USB.

Article 12 – Utilisation de la messagerie électronique

Les adresses mails sont soit nominatives soit partagées.
Les possesseurs d'une adresse mail nominative sont les seuls propriétaires de cette adresse et ne peuvent en aucun cas communiquer leurs codes de connexion à un tiers.
La messagerie peut être déléguée à un collaborateur, y compris durant un temps de présence du titulaire de la messagerie.
En cas d'absence prévue de l'agent, congés, formation…, il est demandé à l'agent d'activer un message automatique d'absence dans les paramètres de sa messagerie afin de pallier tout retard ou défaut d'informations, qui pourrait porter préjudice à l'image de la collectivité.
L'utilisation du courrier électronique à des fins personnelles est tolérée dans des proportions raisonnables et à la condition de ne pas affecter le trafic normal des messages professionnels.
Il est recommandé de créer un dossier personnel dans sa boite mail pour y ranger tout ce qui se rapporte à la vie personnelle de l'agent afin que ce dossier puisse être retiré dans le cas où l'agent devrait laisser l'accès de sa messagerie à un autre collaborateur.

Face aux risques de cyberattaques, il est demandé aux agents d'être vigilant avant d'ouvrir une pièce jointe ou de cliquer sur un lien sans que l'expéditeur soit approuvé et connu et que vous attendiez un message de sa part.

Article 13 – Utilisation d'internet

Tout utilisateur est responsable de l'utilisation qu'il fait d'internet (et de toutes ressources informatiques de façon générale) ainsi que du contenu de ce qu'il affiche, télécharge ou envoie. Il doit en permanence garder à l'esprit que c'est sous le nom de la collectivité qu'il se présente sur internet et doit se porter garant de son image.

Chaque utilisateur doit prendre conscience qu'il est dangereux pour la collectivité :

- de communiquer à des tiers des informations techniques concernant son matériel ;
- de diffuser des informations sur la collectivité via des sites internet (hormis les sites de la collectivité).

L'utilisation d'Internet devra respecter la législation française.
Le rappel non exhaustif des règles de droit principalement concernées par l'utilisation d'Internet et du Service de messagerie proposés vise le double objectif de sensibiliser l'utilisateur à leur existence et à leur respect et de renforcer ainsi la prévention d'actes illicites.
Outre l'atteinte aux valeurs fondamentales régissant la vie en société, dont en particulier les principes de neutralité religieuse, politique et commerciale, sont également (mais pas exclusivement) interdits et le cas échéant sanctionnés par voie pénale :

- l'atteinte à la vie privée d'autrui (article 226-1 et 226-7 du code pénal) ;
- la diffamation et l'injure ;
- la provocation de mineurs à commettre des actes illicites ou dangereux, le fait de favoriser la corruption d'un mineur, l'exploitation à caractère pornographique de l'image d'un mineur, la diffusion de messages à caractère violent ou pornographique susceptibles d'être perçus par un mineur ;
- l'incitation à la consommation de substances interdites ;
- la provocation aux crimes et délits et la provocation au suicide, la provocation à la discrimination, à la haine notamment raciale, ou à la violence ;
- l'apologie de tous les crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité ; la négation de crimes contre l'humanité ;
- le fait d'effectuer des opérations nuisibles au bon fonctionnement du matériel, le fait d'installer des programmes personnels, le fait de modifier en quoi que ce soit la configuration du poste (article 323-1 à 323- 7 du code pénal sur la fraude informatique).

Si toutefois dans le cadre d'une recherche à partir d'une arborescence, de mots-clefs, le résultat de celle-ci amenait l'utilisateur à pointer sur des sites des pages ou des forums dont le titre et/ou les contenus constituent une infraction à la loi française, l'utilisateur devra immédiatement interrompre la consultation du site concerné sauf à encourir les sanctions prévues par la législation en vigueur et à répondre des actions en justice initiées à son encontre.

L'utilisation d'internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel et l'intégrité du système d'informations de la collectivité.

Article 14 – Utilisation de la téléphonie fixe

L'utilisation de la téléphonie fixe à des fins privées est tolérée dans des limites raisonnables et à condition qu'elle n'entrave pas la bonne réalisation de vos missions.
Pour appeler l'extérieur, merci d'ajouter le 0 avant de composer le numéro.

Article 15 – Utilisation de la téléphonie mobile

L'agent disposant d'un smartphone professionnel doit obligatoirement mettre un code de déverrouillage sur son téléphone pour des raisons de sécurité.
L'installation d'application de réseaux sociaux non européens (Tik Tok, Instagram, …) est fortement déconseillée, en dehors des missions de l'agent, ceux-ci ne respectant les lois de la RGPD. (Patriot Act…).
Veillez au droit à l'image lors de la prise de photo justifiée par vos missions.

Article 16 – Utilisation des dispositifs personnels

Vous êtes autorisé à connecter vos comptes professionnels sur vos équipements personnels (exemple : messagerie professionnelle sur téléphone personnel).
Merci de prendre note que vous êtes responsables de la sécurisation de ceux-ci.

Article 17 – Utilisation des outils collaboratifs

Dans le cadre de la mise en place de Teams, la DSIT a mis à disposition des équipes collaboratives par direction.
Il est possible de demander à la DSIT la création d'équipe pour les besoins d'un projet transversal.
Il vous sera demandé lors de la création d'une équipe sur teams la durée de conservation des données.
Les données sur Teams sont stockées sur des Datacenter français et respectent donc la RGPD.

Article 18 – Droit à la déconnexion

La collectivité s'engage à contribuer à une articulation optimale entre la vie personnelle et la vie professionnelle de chaque collaborateur pour l'utilisation des technologies actuelles et futures.
Les outils numériques (ordinateurs, téléphones et/ou tout support multimédia rentrant dans cette catégorie) mis à disposition des agents par la collectivité à des fins professionnelles sont susceptibles d'être utilisés en dehors des horaires de travail.
La collectivité rappelle à ses agents qu'il n'existe pas d'obligation liée à l'utilisation des outils hors des horaires indiqués dans leurs contrats de travail.
Si l'utilisation des outils numériques peut être effectuée hors des horaires de travail, la collectivité recommande à l'ensemble de ses agents de veiller à ne pas faire une utilisation qui porterait une atteinte manifeste à l'équilibre entre leur vie personnelle et leur vie professionnelle.

Article 19 – Droit de reproduction

Chaque utilisateur ne doit pas copier un logiciel pour l'utiliser sur un autre poste ou en dehors de son lieu de travail. Les copies de sauvegarde de logiciels, prévues par le code de la propriété intellectuelle sont exclusivement réalisées par la DSIT. Des droits de reproduction existent également pour les œuvres littéraires, musicales, photographiques, audiovisuelles qui ne doivent en aucun cas être téléchargées reproduites ou diffusées sans autorisation de l'auteur ou du propriétaire des droits d'exploitation.
Chaque agent veillera à respecter les règles de protection du droit d'auteur en ne se rendant pas coupable de contrefaçon :

- à l'occasion d'un téléchargement de données (marque, son, image, texte …) depuis un site internet ;
- en faisant une copie d'un logiciel commercial pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle ;
- en photocopiant sans autorisation des documents protégés (articles de presse, livres …) à des fins autres que privées.

Modalités de l'assistance de la DSIT

Article 20 – Procédures informatiques

L'ensemble des procédures informatiques à destination des agents est sur le Commun Q:\procedures informatiques.
Avant de créer un ticket GLPI pour intervention de la DSIT, merci de vous y référer.
Tout déménagement doit faire l'objet d'une demande préalable à la DSIT via un ticket GLPI afin de vérifier les disponibilités techniques des locaux et ensuite de procéder au câblage et paramétrage du réseau LAN et téléphonique.

Article 21 – Déclarer un incident ou une demande

Toute déclaration d'une demande ou d'un incident doit faire l'objet d'un ticket GLPI afin d'être catégorisé et priorisé par la DSIT, GLPI permet de garantir une traçabilité et un suivi de tous les tickets.

GLPI est le point d'entrée de l'ensemble des demandes et incidents informatique, les appels aux agents sont strictement réservés aux urgences. (impact sur le service à l'usager, impact sur toute une direction…)

La DSIT assure un accueil physique et téléphonique à minima du lundi au vendredi de 08h30 à 12h30 et de 13h30 à 17h30.

Lorsque vous rencontrez un dysfonctionnement avec votre matériel ou un logiciel ou pour tout autre besoin d'information ou demande d'évolution, vous pouvez enregistrer votre demande en vous connectant à GLPI (ouvrir le raccourci Google : Déclaration incidents – DSIT) avec vos identifiants de connexion Windows et cliquer sur l'onglet « créer un ticket » en haut de la page.

GLPI est accessible à l'adresse suivante : glpi.territoiresvendomois.fr

Toutes les informations dont le service informatique a besoin sont pré-remplies et il vous suffit de compléter le ticket et de le valider.

Rappelons que GLPI est accessible à partir de n'importe quel navigateur internet à l'adresse glpi.territoiresvendomois.fr : vous pouvez donc créer une demande depuis votre smartphone ou ordinateur personnel si vous êtes en difficulté en situation de télétravail par exemple.
Les directeurs/trices des services doivent formuler leurs demandes budgétaires via GLPI pour leurs collaborateurs/trices. Tout agent doit donc formuler ses demandes à son/sa directeur/trice pour qu'il/elle formule la demande auprès de la DSIT.
Pour toutes demandes de dépannage de petits matériels (souris, clavier, câble, casque audio) il n'est pas nécessaire de demander aux directeurs/trices des services de faire le ticket, tout agent peut formuler cette demande directement.

Article 22 – Déclarer l'arrivée d'un nouvel agent

Avant qu'un agent (titulaire, contractuel, stagiaire, …), utilisateur du système d'information, intègre la collectivité, le gestionnaire recrutement (Direction des ressources humaines) adresse au N+1 de l'agent en question une fiche d'accueil dans laquelle un formulaire informatique doit être complété et renvoyé aux personnes en copie du premier courriel.
Cet envoi doit se faire dans un délai raisonnable (minimum quinze jours) avant l'arrivée de l'agent afin que la direction informatique ait le temps de mettre en œuvre les modalités de son arrivée.

Une fois que le service informatique réceptionne par courriel la fiche d'arrivée de l'agent, un ticket GLPI est créé par la DSIT dans lequel apparaît l'ensemble des tâches à faire pour accueillir l'agent dans les meilleures conditions. Il n'est donc pas nécessaire à la direction de créer le ticket.

A chaque fois qu'une tâche est effectuée une notification GLPI arrive par courriel à la personne qui a envoyé la fiche d'accueil au service informatique. Ladite personne peut donc aller consulter l'état d'avancement du ticket.

Article 23 – Déclarer le départ d'un agent

Lorsqu'un agent quitte la collectivité, son N+1 doit en informer la DSIT en créant un ticket GLPI et en sélectionnant dans catégorie : AGENT – DEPART.
Le ticket se pré-rempli dès qu'on choisit cette catégorie, il suffit donc ensuite de le compléter.
Lors du départ d'un collaborateur, il doit être indiqué via le ticket GLPI ce qui doit advenir des fichiers et courriers électroniques de l'utilisateur et/ou, s'il faut rediriger la boite mail vers un autre collaborateur.
Lorsque le ticket de départ d'un agent est créé la personne à l'origine du ticket recevra par courriel les notifications d'avancement des tâches du ticket.
Cette étape est cruciale pour la sécurité du système d'information, ne pas prévenir la DSIT revient à laisser des accès ouverts à notre système et met en danger la collectivité.
Les supérieurs hiérarchiques des agents qui quittent la collectivité sont responsables du retour des outils informatiques mis à leurs dispositions.

Nous vous rappelons que les données (fichiers, email…) de l'agent partant appartiennent à la collectivité et ne doivent en aucun cas être supprimés par l'agent avant son départ sans la validation de son supérieur hiérarchique.

Article 24 – Réserver une ressource

Lorsque vous avez besoin d'un prêt de matériel (pc portable, vidéoprojecteur, micro Jabra) vous devez vous connecter à Outlook, créer une réunion et ajouter le matériel souhaité dans les participants. La disponibilité du matériel est accessible via l'« assistant planification ». Pour réserver une salle de réunion, la procédure est identique.

La réservation de ressource est automatiquement acceptée si elle est disponible à l'exception de la salle de réunions aile Saint-Jacques, qui sera soumise à validation de la direction générale.

Aucun matériel ne sortira du parc sans qu'un agent de la DSIT soit présent et autorise sa sortie.

Les horaires de récupération du matériel sont du lundi au vendredi de 9h30h à 12h et de 13h30 à 17h.

Article 25 – Accès Données d'un agent absent

Pour assurer une continuité dans l'activité professionnelle, l'employeur peut être amené à accéder aux données, mails et fichiers, d'un agent absent.
Les tribunaux considèrent que tout message reçu ou envoyé depuis le poste de travail mis à disposition par l'employeur a par principe un caractère professionnel. Dans ce cas, l'employeur peut le consulter. Toutefois, si le message est clairement identifié comme étant personnel, par exemple, si l'objet du message précise clairement qu'il s'agit d'un message privé ou personnel, l'employeur ne doit pas en prendre connaissance. Il doit respecter le secret des correspondances.

La procédure à suivre :

- un responsable hiérarchique ou RH doit prévenir de manière écrite, SMS/Mail/Courrier, à l'agent absent que telle personne, la nommer, va accéder à ces données sur son ordinateur, qu'elle aura un accès à ses mails, qu'un routeur de courrier va être mis en place ;
- un responsable hiérarchique ou RH prévient ensuite la DSIT qu'elle peut générer un mot de passe temporaire sur la session de la personne absente, créer le routeur de courrier en mentionnant le message souhaité, faire une délégation de la boite mail ;
- la DSIT communique le nouveau mot de passe à la personne qui accédera à ces données ;
- la personne qui accédera à ces données copie/colle les données de l'ordinateur vers le réseau. Elle pourra accéder aux mails de la personne absente de son poste. Elle s'engage à respecter le secret des correspondances de la personne absente ;
- la personne qui accédera à ces données prévient la DSIT de remodifier le mot de passe ;
- un responsable hiérarchique ou RH veillera à communiquer au retour de la personne toutes les informations récupérées.

Article 26 – Télétravail

Le télétravail sous charte est en vigueur au sein de la collectivité depuis février 2022.
Si vous souhaitez faire du télétravail, vous devez prendre connaissance de la charte en vigueur et remplir le formulaire pour validation par l'autorité administrative et enregistrement par la DRH.
Une fois le formulaire validé, vous pouvez faire un ticket GLPI pour que la cellule technique vous configure une connexion à distance et vous ouvre les droits nécessaires.

Si vous disposez au sein de la collectivité d'un pc portable, vous pourrez emmener cet ordinateur chez vous pour faire du télétravail.

Les personnes disposant de matériel fixe seront obligées de laisser leur ordinateur allumé la veille du télétravail sauf si un collègue peut démarrer votre ordinateur le matin.
Si vous rencontrez des difficultés à vous connecter à distance durant un jour de télétravail et que vous avez vérifié que vous disposez d'une connexion internet suffisante chez vous (que votre pc à distance est bien allumé si vous avez un pc fixe), merci de bien vouloir créer un ticket GLPI.

Pour rappel, sauf ordinateur portable, aucun autre matériel du bureau ne doit être transporté chez vous dans le cadre de vos missions.
Le service informatique ne sera pas responsable de la casse ou de l'usure prématurée du matériel personnel.
La DSIT ne fournira pas d'équipements supplémentaires (écrans…,) pour télétravailler.

Modalités d'application de la stratégie numérique responsable

Article 27 – Bonnes pratiques sur la messagerie

Afin de limiter notre empreinte numérique il est demandé à tous les agents de bien vouloir :

- limiter l'envoi des mails (privilégier les échanges directs ou téléphoniques ou le mode conversation dans Teams) ;
- trier et supprimer les mails (notamment ceux contenant des documents volumineux) ;
- se désabonner des newsletters qui ne vous servent pas ;
- limiter le nombre de personne en copie des mails ;
- limiter l'envoi des pièces jointes (en interne -> privilégier l'envoi du chemin d'accès au document) ;
- bloquer un expéditeur spam pour ne plus recevoir ses mails (clic-droit sur le mail dans la boîte de réception ou indésirable, choisissez bloquer puis bloquer l'expéditeur) ;
- vider la boîte de courrier indésirable ;
- vider la corbeille ;
- limiter l'utilisation du répondre à tous lorsque ce n'est pas nécessaire.

Accusé de réception en préfecture
041-214102691-20230920-VVSG20230920-16-AR
Date de télétransmission : 29/09/2023
Date de réception préfecture : 29/09/2023

Article 28 – Bonnes pratiques de navigation sur Internet

Lors de la préparation des postes informatiques il sera automatiquement installé sur le navigateur un moteur de recherche appelé Ecosia afin de rendre la navigation sur ces postes plus vertueuse.
Ecosia est un moteur de recherche écologique qui plante des arbres grâce à ses revenus publicitaires reversés à 80 % à des projets de reforestation dans le monde. A ce jour, plus de 160 millions d'arbres ont été plantés.
Ecosia neutralise 100% des émissions de CO2 (Dioxyde de carbone) de ses serveurs, de son infrastructure, de ses locaux et des appareils de ses utilisateurs grâce à un projet de compensation carbone géré par son partenaire Myclimate.
Sont concernés par leur projet : le désert du Burkina, Madagascar, Pérou…
Privilégier la mise en favoris des pages de navigation consultées régulièrement permet d'éviter de retaper ses recherches et induit non seulement un gain de temps mais aussi une limitation des émissions de GES (gaz à effet de serre).

Article 29 – Bonnes pratiques d'impression

Notre environnement est fragile, merci de n'imprimer qu'en cas de réelle nécessité, le double écran peut permettre de pallier ces impressions et le bureau Projet peut vous aider à dématérialiser vos flux.
Merci de privilégier les copies N&B et les impressions en recto verso.

Article 30 – Bonnes pratiques sur l'ensemble des équipements informatiques

Eteindre l'ensemble des équipements, écrans, ordinateurs, copieurs… avant de partir le soir.

Article 31 – Bonnes pratiques sur la téléphonie fixe

Lorsque vous téléphonez à un collaborateur en interne, merci d'utiliser le diminutif du numéro, ce type d'appel n'étant pas facturé (par exemple : au lieu de 02 54 89 42 51 appelez le 42 51).

Article 32 – Bonnes pratiques de stockage

Il est important de rappeler que les documents de travail, les versions intermédiaires doivent être régulièrement supprimées pour ne pas consommer inutilement de ressources informatiques et baisser nos coûts de stockage.
Les photos stockées sur le réseau doivent être compressées pour les mêmes raisons et supprimées lorsqu'elles sont devenues inutiles (voir procédure de compression), de même que les plans et autres documents volumineux.

Modalités d'application de la présente charte

Article 33 – Responsabilités et sanctions encourues en cas de non-respect de la charte informatique

L'utilisateur doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n° 84 -53 du 26 janvier 1984 relative à la fonction publique territoriale.
Les manquements aux règles édictées par la présente charte peuvent engager la responsabilité de l'utilisateur et entraîner des sanctions disciplinaires à son encontre.
L'administration territoriale se réserve également le droit d'engager ou de faire engager des poursuites administratives, indépendamment des sanctions disciplinaires mises en œuvre, en cas de non-respect de la charte informatique.

Article 34 – Condition de mise en œuvre de la charte

Circuit de validation interne :

- comité social territorial + F3SCT ;
- autorité territoriale par arrêté.

Circuit de mise en œuvre :

- annexion au « Règlement intérieur hygiène et sécurité ».

Article 35 – Bilan annuel en F3SCT et Processus de révision

Un bilan annuel sur le respect de la charte informatique sera présenté en F3SCT.

La charte pourra être révisée en raison des évolutions technologiques et règlementaires, à la demande de la collectivité ou tout autre autorité ci-dessus citée. Elle sera alors applicable après respect des mêmes procédures d'approbation.