AR CONTROLE DE LEGALITE : 072-200072684-20260212-2026_02_031-DE
en date du 26/02/2026 ; REFERENCE ACTE : 2026_02_031
Publié le : 04/03/2026

Recommandations

Charte d'utilisation des moyens informatiques et des outils numériques

Gesnois Bilurien
COMMUNAUTÉ DE COMMUNES

Liste de révision

Version	Date	Commentaires	Auteur	Contrôleur	Approbateur
1	31/10/2025	Création du document	TGS France		
2					
3					
4					

Table des matières

Préambule

La présente Charte d'utilisation du système d'information définit les règles d'usage, de sécurité et de responsabilité applicables à l'ensemble des agents, élus, stagiaires et prestataires de la **Communauté de Communes du Gesnois Bilurien.**

Elle complète le règlement intérieur de la collectivité et participe à la démarche de sécurisation de son système d'information, dans le respect :

- Du Règlement Général sur la Protection des Données (RGPD) et de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
- Du Référentiel Général de Sécurité (RGS) et des recommandations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ;
- Des préconisations de la CNIL et des bonnes pratiques en matière de sécurité numérique dans le secteur public local.

La Communauté de Communes du Gesnois Bilurien s'est dotée d'un système d'information permettant à ses services d'assurer la continuité et la qualité du service public sur l'ensemble du territoire. Ce système comprend notamment :

- Un réseau informatique et téléphonique (administratif, technique, enfance-jeunesse, école de musique, EPN, etc.) ;
- Un Drive communautaire sécurisé (Nextcloud) utilisé pour le partage, le stockage et la collaboration documentaire ;
- Un ensemble d'applications métiers (Berger-Levrault, iNoé, iMuse, iParapheur Libriciel, GestSup…) ;
- Des comptes OVH pour la messagerie professionnelle ;
- Des équipements mobiles mis à disposition des agents et élus.

L'objectif de la présente charte est de :

- Favoriser un usage responsable et sécurisé des outils numériques mis à disposition ;
- Protéger les données de la collectivité, des administrés et des partenaires ;
- Prévenir les incidents liés à la perte, au vol ou à l'utilisation inappropriée des équipements ou des informations ;
- Garantir la conformité réglementaire et la continuité du service public.

Contexte et engagement collectif

Depuis sa création en 2017, **la Communauté de Communes Le Gesnois Bilurien** s'est engagée dans une modernisation progressive de son système d'information, soutenue par :

- La structuration des accès utilisateurs (procédure d'ouverture, authentification forte par OTP, politique de mot de passe) ;
- Le déploiement d'un Drive sécurisé à double authentification ;
- La formalisation des droits d'accès par service et par profil ;
- La mise en place d'outils de support et de gestion d'incidents (GestSup) ;
- La sensibilisation continue des agents et des élus à la cybersécurité.

Cette charte vise à renforcer la culture de sécurité et de confiance numérique au sein de la collectivité. Chaque utilisateur du système d'information est acteur de la sécurité et s'engage à adopter un comportement professionnel, éthique et prudent, au service de la collectivité et des citoyens.

Valeur juridique

La présente charte a valeur d'engagement individuel.

Elle doit être lue, comprise et signée par tout utilisateur avant toute attribution d'un compte ou d'un accès aux outils informatiques.

Elle constitue un document annexe au règlement intérieur de la Communauté de Communes et s'impose à tous ses utilisateurs, internes ou externes, dans le cadre de leurs missions.

1. Définition des termes

Il est entendu par :

1.1. Système d'Information

Ensemble coordonné de moyens humains, matériels, logiciels et organisationnels permettant d'élaborer, traiter, stocker, transmettre, sauvegarder et présenter l'information nécessaire au fonctionnement de la collectivité.
Le Système d'Information de la Communauté de Communes du Gesnois Bilurien inclut les réseaux internes, les serveurs, le Drive communautaire, les postes informatiques, les outils de communication et les applications métiers.

1.2. Ressource informatique

Les serveurs informatiques, les ordinateurs, micro-ordinateurs, mini-ordinateurs, postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, de sauvegarde, de reproduction, d'impression, de transmission, de réception et de traitement de l'information et tout équipement de télécommunication, les logiciels, progiciels, didacticiels, banques de données et d'informations (textuelles, sonores, symboliques ou visuelles) placées dans un équipement ou sur un média informatique, système de courrier électronique et système de messagerie vocale, dont la collectivité est propriétaire ou locataire, ou sur lesquels elle possède un droit d'utilisation.

1.3. Système de courrier électronique

Service destiné au grand public permettant d'échanger entre Utilisateurs tout message sous forme de texte, de son ou d'image et des documents numériques via Internet. Les services de messagerie instantanée (ou de dialogue en ligne) et les forums de discussion ne sont pas considérés comme des Services de courriers électroniques.

1.4. Utilisateur

Toute personne utilisant le système d'information. L'utilisateur peut être une personne physique mais également une machine automatique (Robot / Bot)

1.5. Utilisateur avec privilèges

Utilisateur du système d'information, a qui certains rôles ou droits spécifiques supplémentaires ont été attribués.

1.6. Administrateur

L'administrateur est une personne du service informatique, ou à défaut le(s) prestataire(s) lié(s) par un contrat, qui a la responsabilité de gérer le ou les serveurs de la collectivité, l'infrastructure technique et le bon fonctionnement du système d'information. Celui-ci possède un niveau de droit élevé.

1.7. Moyen d'authentification

Élément qui est généralement connu ou possédé uniquement par l'utilisateur et qui permet de l'authentifier de manière unique (comme un mot de passe, une clé privée d'un certificat électronique, etc.). Il s'agit d'une preuve utilisée pour démontrer son identité.

1.8. Données

Représentation d'une information contenue dans un programme informatique.

1.9. Données à caractère personnel

Toute information se rapportant à une personne physique identifiée ou identifiable.

1.10. Traitements informatiques

Par traitement des données, on entend le recours à différents procédés : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement.

1.11. Réseau

Le réseau informatique est constitué de tous les éléments permettant l'interconnexion des ressources informatiques : Eléments actifs (commutateurs, pare-feu, points d'accès Wifi, routeurs), les connexions Internet et GSM.

2. Champs d'application

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de la collectivité, quel que soit leur statut, y compris les élus, agents et intervenants extérieurs.

2.1. Moyens et outils mis à disposition

Les ressources informatiques, logicielles et de télécommunication mises à disposition par la Communauté de Communes du Gesnois Bilurien ont pour unique finalité l'exercice des missions de service public.

Elles comprennent notamment :

- les postes de travail (fixes ou portables), imprimantes, copieurs et périphériques ;
- les terminaux mobiles professionnels (tablettes, téléphones) ;
- les réseaux internes, accès Wi-Fi et connexions VPN ;
- les serveurs hébergeant les applications métiers ;
- le Drive communautaire Nextcloud pour le partage documentaire ;
- la messagerie professionnelle OVH / Microsoft 365 ;
- les logiciels et progiciels métiers (Berger-Levrault, iNoé, iMuse, iParapheur Libriciel, GestSup, etc.) ;
- les services collaboratifs ou de visioconférence autorisés par le responsable SI.

Ces outils demeurent la propriété exclusive de la collectivité, qu'ils soient achetés, loués ou mis à disposition par un prestataire.

Ils doivent être utilisés dans le strict cadre professionnel et dans le respect des règles de sécurité définies par la présente charte.

Toute installation, suppression ou modification d'un équipement ou d'un logiciel doit être validée par le service informatique ou par son prestataire désigné.

2.2. Connexions au système d'information à distance

L'accès à distance au système d'information est autorisé pour :

- les agents habilités au télétravail ou à la mobilité professionnelle ;
- les administrateurs et prestataires dans le cadre d'opérations de maintenance ou de support ;
- les élus disposant d'un espace documentaire ou de messagerie dédié.

Ces accès doivent s'effectuer exclusivement via :

- un réseau VPN sécurisé ou un canal chiffré (SSL/TLS) ;
- une authentification forte (identifiant, mot de passe complexe et OTP) ;
- et des équipements conformes aux exigences de sécurité de la collectivité

L'utilisateur s'engage à :

- ne jamais utiliser de connexion publique non sécurisée pour accéder aux outils communautaires ;
- verrouiller sa session en cas d'absence ou d'inactivité ;
- signaler sans délai toute anomalie ou tentative d'accès suspecte.

2.3. Dérogations

Toute demande de dérogation aux différents éléments définis dans le cadre de la présente Charte doit être présentée par écrit au service SI qui se réserve le droit d'accepter ou de refuser les demandes de dérogation.

3. Droits et devoirs des utilisateurs de la collectivité

L'accès au Système d'Information (SI) implique une responsabilité individuelle de chaque utilisateur.
Tout agent, élu, stagiaire ou prestataire contribue, par son comportement, à la sécurité, la fiabilité et la continuité du service public numérique.

3.1. Utilisateurs

Chaque utilisateur :

- s'engage à utiliser les ressources informatiques exclusivement à des fins professionnelles liées à ses missions au sein de la collectivité ;
- veille à préserver la confidentialité des informations auxquelles il a accès (données administratives, comptables, sociales, techniques, etc.) ;
- respecte les procédures internes (accès, mot de passe, sauvegardes, signalement d'incidents) ;

- protège son environnement de travail (écran verrouillé, documents sensibles rangés, mot de passe non divulgué) ;
- et informe sans délai le responsable informatique de toute anomalie, perte, vol ou suspicion de compromission.

L'utilisateur reconnaît que :

- les équipements, logiciels et données traitées sur le SI appartiennent à la Communauté de Communes ;
- aucune donnée personnelle, privée ou sensible ne doit être stockée dans les répertoires professionnels (Drive, messagerie, poste de travail) sans autorisation ;
- l'usage d'Internet, du Wi-Fi et de la messagerie professionnelle est soumis à un principe de sobriété, de loyauté et de respect du cadre public.

L'utilisateur est tenu de signaler immédiatement :

- tout incident ou dysfonctionnement via l'outil GestSup ou par contact direct avec le service informatique ;
- tout courriel suspect, tentative d'hameçonnage (phishing) ou fichier inhabituel reçu par messagerie.

3.2. Cas des administrateurs et utilisateurs avec pouvoir

Les administrateurs et utilisateurs disposant de privilèges particuliers (accès aux serveurs, gestion des comptes, paramétrages réseau, etc.) sont soumis à des obligations renforcées :

- leurs comptes à privilèges sont nominatifs, tracés et distincts de leurs comptes utilisateurs standards ;
- toute action sensible (création, suppression, modification d'accès, configuration de sauvegarde, etc.) doit être documentée et consignée dans un journal d'intervention ;
- ils veillent à ne jamais divulguer d'informations techniques (adresses IP, mots de passe, codes OTP, configurations internes) en dehors du cercle autorisé ;

Les administrateurs agissent au nom et pour le compte de la collectivité, sous la responsabilité du Directeur Général des Services (DGS) et du référent informatique.

Toute négligence ou intervention non autorisée peut engager leur responsabilité personnelle et donner lieu à des sanctions disciplinaires ou contractuelles.

3.3. Obligations des prestataires extérieurs à des fins de maintenance ou d'administration

Afin d'encadrer les interventions des prestataires informatiques de la collectivité, à des fins de maintenance ou d'administration du Système d'Information, il sera nécessaire de suivre les règles suivantes :

- Prévenir en amont de l'intervention le responsable informatique (Nature de l'intervention, Personnel intervenant, Durée prévisionnelle de l'intervention)
- Avertir sans délai la collectivité des dysfonctionnements graves, de failles de sécurités constatées.
- Fournir un compte rendu d'intervention.
- Se conformer aux exigences et obligations de la présente charte.

4. Confidentialité

4.1. Accès aux ressources du système d'information

4.1.1. Les moyens d'authentification utilisés par la collectivité

L'accès aux ressources numériques (postes, serveurs, Drive, applications métiers, messagerie, etc.) est :

- strictement individuel et nominatif ;
- accordé sur la base du principe du moindre privilège, c'est-à-dire limité aux seuls outils et données nécessaires à la mission de l'utilisateur ;
- encadré par une procédure d'habilitation gérée par le service informatique, sur demande validée par le supérieur hiérarchique.

Chaque utilisateur s'engage à :

- protéger ses moyens d'authentification (identifiant, mot de passe, clé d'accès, code OTP) et à ne jamais les partager, même temporairement ;
- verrouiller son poste ou fermer sa session en cas d'absence, même de courte durée ;
- ne pas tenter d'accéder à des informations, répertoires ou applications auxquels il n'a pas été autorisé à accéder.

Le non-respect de ces règles constitue une violation de la confidentialité et peut entraîner des sanctions disciplinaires ou pénales.

4.1.2. Conditions d'accès aux locaux techniques

L'accès aux locaux techniques est réservé aux intervenants techniques et aux prestataires.

La demande d'accès doit être effectuée auprès du responsable informatique.

4.1.3. Modalités d'accueil d'un nouvel agent

A l'arrivée d'un nouvel agent, il lui sera remis le règlement intérieur de la collectivité et ses annexes dont la charte informatique afin de l'informer des modalités d'utilisation des moyens informatiques et outils numériques.

4.1.4. Modalité de départ d'un agent

Lorsque la collectivité retire à l'utilisateur son privilège d'accès et d'utilisation des ressources informatiques pour quelque raison que ce soit, il doit :

i. Fournir à l'administrateur ou aux prestataires tous ses codes d'accès et mots de passe de sorte qu'ils soient désactivés ;

ii. Supprimer les informations, les données et les programmes personnels qu'il a stockés par le biais de son code d'accès. Les données professionnelles devront être restituées à la collectivité ;

iii. Donner accès à toutes autres informations, données et programmes qu'il a stockés par le biais de son code d'accès.

iv. Si l'utilisateur néglige de prendre les mesures nécessaires à l'égard de ce qui est visé à l'alinéa « ii », ces informations, données et programmes seront considérés périmés 15 jours après la date du retrait du privilège et la collectivité aura le droit de les supprimer sans que l'utilisateur puisse s'en plaindre ou tenir la communauté de communes responsable de leur perte.

v. Les paragraphes « i » et « iv » s'appliquent aussi lorsqu'une personne perd sa qualité d'utilisateur autrement que par le retrait de son privilège.

4.1.5. Mot de passe

4.1.5.1. Accès au système d'information

Les mots de passe des comptes utilisateurs permettant l'accès au système d'information sont régis par une stratégie qui impose des règles à leur création et à leur modification, à savoir :

- 12 caractères minimum
- Doit être composé de chiffres, lettres, majuscules, caractères spéciaux
- Doit être renouvelé tous les 6 mois
- Ne peut reprendre les 5 mots de passe précédents.

4.1.5.2. Accès au Wifi

L'accès au Wifi de la collectivité est strictement réservé aux usages des agents et tiers de confiance désignés par la Direction. Il est par conséquent interdit de communiquer à d'autres tiers et d'afficher la clé de sécurité du réseau WIFI.

4.1.5.3. Accès aux applicatifs :

Les mots de passe des comptes utilisateurs dans les applications doivent respecter les règles établies à l'article 4.1.5.1 de la Charte informatique.

4.1.6. Usage des données de connexion

- Il est formellement interdit de divulguer ses identifiants de connexions.

- Il est formellement interdit de communiquer à des tiers extérieurs de la collectivité, sans autorisation de la direction, la Clé de connexion Wifi ou tout autre accès réseau.
- Il est formellement interdit de tenter de déchiffrer le code d'accès, ou le mot de passe d'un autre utilisateur, ou ceux d'un tiers.
- Il est formellement interdit d'utiliser les codes d'un autre utilisateur pour effectuer ses tâches courantes, même dans le cas où une seconde authentification à un logiciel serait nécessaire.
- Il est formellement interdit d'enregistrer ses mots de passe dans les navigateurs Internet.
- Il est formellement interdit de transmettre son code utilisateur et son mot de passe ou tout autres identifiants de connexion par mail. Dans le cas où il serait nécessaire de transférer des informations de connexions, le code utilisateur et le mot de passe devront être envoyé par deux canaux distincts, exemple : Mail + SMS / Mail + Courrier postal.
- Il est formellement interdit d'écrire votre code d'accès sur un support papier (post-it, feuille A4, …).

4.1.7. Verrouillage de son poste informatique

En cas d'absence devant son poste de travail, et en l'absence de dispositif de verrouillage automatique, il convient de verrouiller sa session.

Un verrouillage rapide peut être réalisé dans Windows 11 par l'utilisation du raccourci clavier : « **+ L** »

4.1.8. Utilisation des données

- Ne pas accéder, tenter d'accéder, ou supprimer des informations si cela ne relève pas des tâches incombant à l'utilisateur
- Ne pas stocker de données professionnelles sur des supports amovibles non sécurisés.
- Ne pas stocker ou transférer de données professionnelles sur des environnements Cloud non sécurisés et non validées par la direction.

Les exports de données des différents logiciels ne peuvent être réalisés que dans un but professionnel, et strictement encadrés. Une attention toute particulière devra être portée si ces exports intègrent des données à caractère personnel.

4.1.9. Propriété intellectuelle

4.1.9.1. Règle générale

En tout temps, l'utilisateur doit respecter les droits de propriété intellectuelle, notamment les droits d'auteur des tiers.

4.1.9.2. Logiciels, progiciels et didacticiels

Les reproductions de logiciels, de progiciels ou de didacticiels ne sont autorisées qu'à des fins de copie de sécurité ou selon les normes de la licence d'utilisation les régissant. Seul le service informatique est habilité à réaliser de telle copie.

4.1.9.3. Comportements interdits :

Il est strictement interdit aux utilisateurs :

- D'utiliser toute reproduction illicite d'un logiciel ou d'un fichier électronique ;
- De participer directement ou indirectement à la reproduction illicite d'un logiciel ou d'un fichier électronique ;
- De modifier ou détruire un logiciel, une banque de données ou un fichier électronique, ou d'y accéder sans l'autorisation de son propriétaire ;
- De reproduire la documentation associée à un logiciel sans l'autorisation écrite du titulaire du droit d'auteur de ce logiciel ;
- D'utiliser les équipements et les ressources informatiques et de télécommunications ou le réseau afin de commettre ou de tenter de commettre une infraction aux lois régissant la propriété intellectuelle.
- Utiliser ou connecter des périphériques personnels sur les postes ou le réseau de la collectivité (ex : PC Personnel, Tablette, Smartphones, Clés USB, Disques durs externes...)

5. Usages au sein de l'entité

5.1. Sécurité

5.1.1. Rôle de l'entité

Du fait de la collecte de données et du traitement de celles-ci, **la communauté de communes** s'engage, dans le cadre des dispositions légales et réglementaires qui s'imposent à elle et dans le respect du principe de proportionnalité édicté par le RGPD, à mettre en œuvre toutes les mesures organisationnelles et techniques utiles afin de préserver la sécurité, l'intégrité et la confidentialité des Données, ainsi que la sécurité de son système d'information et de communication, sur le plan technologique et procédural, afin notamment d'empêcher toute modification, tout transfert et toute suppression non-autorisés des Données, et toute intrusion non-autorisée dans son système d'information ou son endommagement.

Par ailleurs, La Direction de la collectivité se réserve, pour quelque raison que ce soit, de manière temporaire ou définitive, le droit d'accorder, de refuser, de modifier ou de supprimer tout ou partie, le droit d'accès de toute personne, prestataire, ou autre tiers, pour des raisons liées directement à la continuité et la sécurité des services.

Toutefois, le premier risque reste le risque humain lié aux traitements et aux manipulations des Données par les Utilisateurs, et par l'utilisation par ces derniers du système d'information et de communication et des outils qui y sont liés. Par conséquent, la mise en place d'outils de sécurité ne doit pas dispenser les utilisateurs de signaler toute tentative d'intrusion extérieure, de falsification ou de présence de virus au responsable des systèmes d'information.

5.1.2. Rôle de l'utilisateur

Le respect de la confidentialité des données est une exigence essentielle.

La protection des missions et du patrimoine informationnel de la collectivité impose à chaque utilisateur une obligation générale et permanente de confidentialité et de secret professionnel, concernant toutes les données et informations mises à sa disposition dans le cadre de son activité professionnelle et de l'utilisation des systèmes d'information.

En conséquence, l'utilisateur s'engage au respect de la présente charte, comme des textes en vigueur et notamment à veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations, conformément aux règles d'éthique professionnelle ou de déontologie, le cas échéant.

Il est interdit d'utiliser des moyens de chiffrement autres que ceux expressément autorisés par le service informatique.

La transmission de données confidentielles ne peut être réalisée qu'aux conditions suivantes :

- Habilitation de l'émetteur ;
- Désignation d'un destinataire autorisé ;
- Respect d'une procédure sécurisée.

Tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des moyens mis à sa disposition et du réseau auquel il a accès, principalement en évitant l'intrusion de virus susceptibles d'endommager le système d'information.

5.1.3. Prestataires de service :

Les prestataires de service qui ont la charge de l'administration des systèmes informatiques de la collectivité sont tenus au secret professionnel et ne doivent pas divulguer des informations ayant un caractère nominatif, de quelque nature qu'elles soient et ce, quel que soit l'ordre hiérarchique.

En aucun cas, les administrateurs ne sont contraints de divulguer ces informations sauf disposition législative et/ou réglementaire particulière en ce sens.

En cas de non-respect de ces dispositions par les administrateurs des prestataires, ceux-ci s'exposent à des sanctions indépendamment des circonstances susceptibles d'engager leur responsabilité.

5.2. Internet

5.2.1. Consultations

L'accès à l'Internet est autorisé au travers du Système d'Information, toutefois, pour des raisons de sécurité l'accès à certains sites peut être limité par des moyens techniques.

En particulier, sont interdits :

- L'utilisation de l'Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives.
- La connexion à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de la collectivité, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information de la collectivité ou engageant financièrement celle-ci.

5.2.2. Usage personnel

L'accès à internet à des fins personnelles dans le cadre professionnel est toléré dans les limites du raisonnable en termes de durée de consultation et d'usage sur la durée des temps de pause.

5.2.3. Réseaux sociaux

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites est interdite ou autorisée sous réserve d'autorisation préalable de la direction de la collectivité. Un tel mode d'expression est susceptible d'engager la responsabilité de la collectivité, une vigilance renforcée des utilisateurs est donc indispensable.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte à la collectivité y compris sur Internet.

5.3. Echanges électronique

5.3.1. Messagerie

Chaque agent peut disposer d'une adresse email pour l'exercice de ses missions. Par principe, tous les messages envoyés ou reçus sont présumés être envoyés à titre professionnel. Par exception, les utilisateurs peuvent utiliser la messagerie à des fins personnelles, dans les limites posées par la loi.

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

5.3.1.1. Usages professionnels

Envoi

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d'informations à caractère confidentiel, de données à caractère personnel ou de données sensibles, ces vérifications doivent être renforcées.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel.

Les messages importants doivent être envoyés avec un accusé de réception ou signés électroniquement.

Réception

L'utilisateur ne doit pas ouvrir, ni répondre à des messages électroniques tels que spam, messages électroniques répétés, ni les transférer lorsque ceux-ci sont reçus à son insu sur leur messagerie électronique professionnelle et ne présentent aucun rapport avec ses fonctions et ses attributions au sein de la collectivité.

Il s'engage, dans pareil cas, à les détruire immédiatement et à avertir le responsable informatique en cas d'abus manifeste de fréquence ou de volume.

Absence

L'utilisateur est informé et accepte qu'en cas d'absence prolongée ou pour la continuité des services, la direction se réserve le droit d'accéder à sa messagerie et à ses dossiers professionnels, et ce sans son consentement préalable.

En cas d'absence, l'utilisateur devra activer la fonction de délégation ou de notification d'absence afin de prévenir toute discontinuité dans le traitement des messages et permettre à ses interlocuteurs de prendre des mesures appropriées.

En cas d'urgence ou pour des raisons liées au besoin de maintenir un niveau de qualité de service, la collectivité peut procéder à la destruction ou réinitialiser les codes d'accès d'un utilisateur.

5.3.1.2. Usages personnels

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte.

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

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

5.3.1.3. Comportements interdits

- D'utiliser dans tous les messages électroniques diffusés sur le réseau, un langage injurieux, malveillant, haineux ou discriminatoire, ainsi que toute forme de harcèlement, de menace ou de diffamation ;
- De capter, de stocker, de reproduire ou de transmettre au moyen du réseau du matériel ou un message à caractère obscène ou pornographique ;
- De procéder au décryptage ou décodage de codes ou de clés d'accès, de fichiers ou de mots de passe, pour quelque raison que ce soit ;
- D'utiliser un ou des subterfuges ou d'autres moyens pour transmettre du courrier électronique de façon anonyme ou au nom d'une autre personne ;
- De réaliser des transferts automatiques de messagerie, vers des messageries personnelles et d'utiliser ces dernières dans le cadre professionnel.

5.4. Bonnes pratiques

L'utilisateur s'engage de respecter à

- Ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ;
- Ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir le responsable informatique.
- Ne pas modifier la configuration de son poste de travail informatique effectuée par le responsable en charge de l'administration du Système d'Information, que ce soit par adjonction, suppression ou modification, sauf exception après accord auprès du service informatique;
- Ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les matériels dont il a usage ;
- Ne pas utiliser (même avec leur accord) ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués où masquer son identité ;
- Ne pas sortir les Equipements informatiques de la collectivité en dehors du site, sauf accord de la Direction ;
- Ne pas télécharger de fichiers, en particulier médias, sans rapport avec l'activité professionnelle ou présentant un risque pour le système d'information ;
- Ne pas utiliser les postes informatiques à des fins de recharge électriques (Object Connectés, Smartphones personnels) ;

5.5. Téléphonie

5.5.1. Usage professionnel

Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un téléphone fixe et/ou mobile, d'un smartphone, ou hot spot wifi.

Les règles édictées dans la présente charte s'appliquent également pour la consultation de sites Internet ou de la messagerie sur des terminaux mobiles (smartphones).

De plus, il est rappelé que l'envoi de SMS engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel.

L'utilisateur est informé qu'un journal des communications, entrantes et/ou sortantes, est accessible par la Direction de la collectivité s'agissant tant de la téléphonie fixe que mobile. Les utilisateurs sont informés que les relevés de communication peuvent faire l'objet d'un contrôle.

5.5.2. Usage Personnel

L'utilisation à caractère personnel du téléphone, fixe ou mobile, est tolérée, à condition qu'elle reste dans des limites raisonnables en termes tant de temps passé que de quantité d'appels.

Les surcoûts pour la collectivité engendrés par l'utilisation de la téléphonie à des fins personnelles devront être remboursés par les utilisateurs concernés. Il s'agit tout particulièrement des appels à des numéros surtaxés et des appels depuis l'étranger ou à destination de l'étranger, au sens de la facturation téléphonique.

Seule la direction pourra avoir accès aux numéros détaillés, permettant d'identifier les interlocuteurs d'un utilisateur, et seulement en cas de différend avec lui.

5.6. Nomadismes / Télétravail

5.6.1. Nomadisme :

5.6.1.1. Avant de partir en mission

- N'utilisez que du matériel (ordinateur, supports amovibles, téléphone) dédié à la mission, et ne contenant que les données nécessaires ;
- Sauvegardez ces données, pour les retrouver en cas de perte ;
- Vérifiez que vos mots de passe ne sont pas préenregistrés.

5.6.1.2. Pendant la mission et/ou en déplacement

- Gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel) ;
- N'utilisez pas les équipements que l'on vous offre si vous ne pouvez pas les faire vérifier par un service de sécurité de confiance ;
- Évitez de connecter vos équipements à des postes qui ne sont pas de confiance. Par exemple, si vous avez besoin d'échanger des documents lors d'une présentation commerciale, utilisez une clé USB destinée uniquement à cet usage et effacez ensuite les données ;
- Refusez la connexion d'équipements appartenant à des tiers à vos propres équipements (Smartphone, clé USB, …) ;
- Ne jamais laisser les appareils de la collectivité sans surveillance ;
- Ne pas utiliser les réseaux Wi-Fi public pour accéder aux données de la collectivité ;
- Informer immédiatement le service informatique en cas de perte ou de vol d'un appareil ;
- L'utilisation d'appareils personnels pour accéder aux données de la collectivité doit être autorisée préalablement par le responsable informatique et doit être conforme aux politiques de sécurité de la collectivité.

5.6.1.3. Après la mission

- Effacez l'historique des appels et de navigation ;
- Changez les mots de passe que vous avez utilisés pendant le voyage ;
- N'utilisez jamais les clés USB qui peuvent vous avoir été offertes lors de vos déplacements (salons, réunions, voyages…) : très prisées des attaquants, elles sont susceptibles de contenir des programmes malveillants.

6. Droit à la déconnexion

6.1. Définition du droit à déconnexion

Le droit à la déconnexion peut être défini comme le droit de l'agent de ne pas être connecté aux outils numériques professionnels et ne pas être contacté, y compris sur ses outils de communication personnels, pour un motif professionnel en dehors de son temps de travail habituel.

Les outils numériques visés sont :

- les outils numériques physiques : ordinateurs, tablettes, téléphones portables, réseaux filaires, etc.
- les outils numériques dématérialisés permettant d'être joint à distance : messagerie électronique, logiciels, connexion wifi, internet/intranet, etc.

Le temps de travail habituel correspond aux horaires de travail de l'agent durant lesquels il demeure à la disposition de la collectivité. Ce temps comprend les heures normales de travail de l'agent et les éventuelles heures supplémentaires. En sont exclus les temps de repos quotidien et hebdomadaire, les temps de congés payés et autres congés exceptionnels ou non, les temps de jours fériés et de jours de repos, les temps d'absences autorisées, de quelque nature que ce soit (absence pour maladie, pour maternité, etc.).

6.2. Mesures visant à garantir le droit à la déconnexion

Aucun agent n'est tenu de répondre à des courriels, messages ou appels téléphoniques à caractère professionnel en dehors de ses heures habituelles de travail, pendant ses congés payés, ses temps de repos et ses absences, quelle qu'en soit la nature.

Il est rappelé à chaque cadre et, plus généralement, à chaque agent de :

- s'interroger sur le moment opportun pour adresser un courriel, un message ou joindre un agent par téléphone ;
- ne pas solliciter de réponse immédiate si ce n'est pas nécessaire ;

- pour les absences de plus de 4 jours, paramétrer le gestionnaire d'absence du bureau sur sa messagerie électronique et indiquer les modalités de contact d'un agent de la collectivité en cas d'urgence ;
- pour les absences supérieures à 15 jours, il pourra également être procédé au transfert des messages électroniques à un autre agent de la collectivité, avec son consentement exprès.

Afin de garantir le droit à la déconnexion des agents, la messagerie électronique professionnelle ne sera plus accessible au salarié dont le contrat de travail est suspendu au-delà d'une absence de 3 semaines.

7. Données à Caractère personnel

7.1. Généralités

La Loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, dite Loi Informatique et Libertés, l'ordonnance n°2018-1125 du 12 décembre 2018, ainsi que le Règlement général sur la protection des données (RGPD) viennent définir les conditions dans lesquelles des traitements de données à caractère personnel peuvent être opérés.

La Loi Informatique et Libertés et le RGPD instituent au profit des Personnes Concernées par les traitements réalisés par les utilisateurs des droits que la présente charte vient protéger et respecter, tant à l'égard des utilisateurs que des tiers.

A cet égard, le Délégué à la Protection des Données (DPO) s'engage d'informer les utilisateurs à :

- ne pas utiliser les données à caractère personnel auxquelles ils peuvent accéder à des fins autres que celles prévues par leurs 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 leurs fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de leurs attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- d'assurer, dans la limite de leurs attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- ne pas accéder, tenter d'accéder ou supprimer les données en dehors de leurs attributions ;
- respecter les droits des personnes concernées (droit d'accès, de rectification, d'opposition, effacement…) conformément aux procédures mises en place par la collectivité;
- en cas de cessation de leurs fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.
- Respecter l'ensemble des procédures liées à la protection des données mises en place par la collectivité et à respecter et favoriser l'ensemble des mesures techniques et organisationnelles mises en place par la collectivité afin de se conformer à la réglementation applicable.

Il convient de rappeler qu'en vertu du Règlement, de la collectivité, le Délégué à la Protection des Données (DPO) et le Responsable de Traitement peuvent être passibles de sanctions importantes, qu'elles soient administratives, civiles ou pénales.

Aussi, le Délégué à la Protection des Données (DPO) s'engage, et par voie de conséquence les utilisateurs, par le respect de la présente charte, à respecter les principes fondamentaux de la protection des données à caractère personnel, à savoir notamment la minimisation de la collecte et la préservation de la confidentialité, de l'intégrité et de la sécurité des données à caractère personnel.

Les utilisateurs sont au cœur de la protection des données à caractère personnel, et par conséquent des libertés et de la vie privée des personnes concernées.

7.2. RGPD

Les agents sont informés que les données à caractère personnel les concernant sont conservées par la collectivité pendant toute la durée de leur relation contractuelle et des délais en matière de prescription.

Conformément à la loi, les utilisateurs sont informés qu'ils disposent d'un droit d'accès et de rectification relatif à l'ensemble des informations les concernant, ainsi qu'il en est fait mention en page 9 de la présente charte concernant les données personnelles à caractère sensible.

Les utilisateurs sont également informés que, pour des motifs légitimes, ils peuvent s'opposer au traitement des données personnelles les concernant.

La communauté de communes Le Gesnois Bilurien est soumise de plein droit au RGPD et à la désignation d'un délégué à la Protection des Données (DPO) et ceci à double titres : d'une part à l'égard de leurs agents et d'autre part à l'égard des citoyens.

La Direction de **La communauté de communes Le Gesnois Bilurien** a donc identifié et désigné un délégué à la Protection des Données (DPO).

La Direction de **La communauté de communes Le Gesnois Bilurien** doit aussi informer ses collaborateurs comme ses clients de leurs droits concernant leurs données personnelles à caractère particulier ou non, et doit aussi recueillir le consentement des collaborateurs comme de salariés.

Elle doit également informer ces derniers des voies de recours définies dans la mise en place du RGPD ainsi que les moyens de contacter le Responsable de Traitement et le délégué à la Protection des Données (DPO).

7.2.1. Le Responsable de traitements (RT)

Il met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au Règlement de l'Union Européenne du 27 avril 2016 relatif au RGPD. Ces mesures sont réexaminées et actualisées si nécessaire. Article 24 alinéa 1 du RGPD.

7.2.2. Le Délégué à la Protection des Données personnelles (DPO)

Les missions du délégué à la protection des données sont au moins les suivantes :

i. Informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les agents qui procèdent au traitement sur les obligations qui leur incombent en vertu du RGPD et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données ;

ii. Contrôler le respect du RGPD, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

iii. Dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35 du RGPD;

iv. Coopérer avec l'autorité de contrôle à savoir la CNIL;

v. Faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet.

Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

8. Conduite à tenir

8.1. Perte ou vol d'un terminal ou d'un support de l'organisation

En cas de perte ou de vol d'un terminal (Smartphone, Ordinateur Portable, …) il est obligatoire de prévenir le service informatique le plus rapidement possible. Le service informatique se réservant le droit et la possibilité de ne pas reconduire le matériel à l'identique.

En cas de perte ou de vol d'un support de l'organisation (clé USB, disque dur externe, …), il est obligatoire de prévenir le service informatique le plus rapidement possible. Le service informatique se réservant le droit et la possibilité de ne pas reconduire le matériel à l'identique.

Il est vivement recommandé de chiffrer les supports amovibles.

8.2. Détection ou suspicion d'une cyberattaque

En cas de détection ou de suspicion d'une cyberattaque ou d'un comportement anormal sur son poste ou sur le réseau informatique de la collectivité, l'utilisateur doit immédiatement informer le responsable informatique et suivre la procédure suivante :

- Débrancher le câble informatique de la ou les machines concernées
- Déconnecter les machines concernées du réseau WIFI
- Ne pas éteindre la ou les machines concernées
- Alerter immédiatement le responsable informatique.

9. Informations et sanctions

L'utilisateur qui contrevient aux dispositions de ce règlement peut être l'objet, en plus des pénalités ou sanctions prévues par les lois et les règlements pertinents, dont ceux de la **communauté de communes Le Gesnois Bilurien** relatifs aux agents, aux élus, aux stagiaires étudiantes ou étudiants, de l'une ou de plusieurs des sanctions administratives suivantes :

vi. La suspension temporaire ou l'annulation de son code d'accès ou de ses mots de passe ;

vii. L'interdiction d'utiliser en totalité ou en partie les ressources informatiques ;

9.1. Absence de responsabilité

La communauté de communes Le Gesnois Bilurien n'assume aucune responsabilité, directe ou indirecte, pour les pertes, dommages ou inconvénients causés aux utilisateurs à l'occasion ou en conséquence de l'utilisation des équipements et des ressources informatiques, de télécommunications, ainsi que du réseau, ou advenant le cas où elle devait, pour quelque cause que ce soit, diminuer ses services, ou les interrompre, quelle que soit la durée de telles diminutions ou interruptions, ou encore arrêter définitivement ses services.

La communauté de communes Le Gesnois Bilurien ne peut en aucun cas être tenu responsable des dommages causés par les informations qu'un utilisateur a véhiculé par l'intermédiaire du réseau ; l'utilisateur demeure seul responsable.

10. Date d'entrée en vigueur

La présente charte est applicable à compter du : …/…/….

Annexe 1 - Activités illégales

Liste d'exemples non exhaustive.

Pornographie juvénile

Avoir en sa possession, télécharger ou distribuer de la pornographie juvénile.

Droit d'auteur

Porter atteinte au droit d'auteur d'autrui sans raison licite.

Diffamation

Faire lire par d'autres un énoncé susceptible de nuire à la réputation de quelqu'un en l'exposant à la haine, au mépris ou au ridicule, ou conçu pour l'insulter.

Piratage et autres crimes contre la sécurité informatique

Utilisation du mot de passe d'autrui pour commettre une fraude ou obtenir de l'argent, des biens ou des services en faisant de fausses représentations sur un système informatique ;

Utilisation non autorisée d'ordinateur et de services informatiques ;

Utilisation, possession ou trafic de mots de passe d'ordinateur volés ou de renseignements relatifs à des cartes de crédit volées ;

Production, possession ou distribution de programmes informatiques conçus pour faciliter l'accès illégal à des systèmes informatiques ;

Méfait concernant des données

Destruction ou falsification de preuves pour faire obstacle à une enquête pénale ;

Vol de service de télécommunication ;

Vol d'équipement informatique.

Harcèlement

Envoyer, sans en avoir l'autorité légale, des messages électroniques incitant quelqu'un à craindre pour sa sécurité ou pour celle de gens qu'il connaît.

Propagande haineuse

Diffuser ou distribuer des messages fomentant la haine ou incitant à la violence.

Interception de communications privées ou de courrier électronique (en transit)

Intercepter illégalement les communications privées de quelqu'un, ou intercepter illégalement le courrier électronique de quelqu'un.

Obscénité

Distribuer, publier ou avoir en sa possession en vue de le distribuer ou de l'exposer publiquement tout document obscène.

Annexe 2 - Activités interdites et nuisibles

Liste d'exemples non exhaustive.

Echange non sécurisé de données

La communication de renseignements protégés ou de données sensibles sur des réseaux non protégés (exemple : wetransfer).

Piratage du Système d'Information

Tenter de percer les dispositifs de sécurité des systèmes informatiques ;

L'insertion et la propagation de virus informatiques ;

Utilisation non autorisée du réseau

Congestionner et perturber les réseaux et les systèmes ;

Gestion de la messagerie

Envoyer des messages abusifs, sexistes, racistes ;

Utilisations détournées

Utiliser les réseaux électroniques de la collectivité pour des affaires commerciales personnelles, pour gain ou profit personnel, ou pour des activités politiques, sans autorisations préalables explicites ;

Destruction de données

La destruction ou la modification de données ou de logiciels ;

Modification de la configuration du réseau

L'utilisation d'une ou plusieurs adresses IP statiques sans autorisation préalable ;

La modification et / ou la manipulation du réseau, équipements et ressources informatiques et de télécommunications, câblage et / ou connections réseaux ;

Droits d'auteurs

L'utilisation des services informatiques, réseau, équipements et ressources informatiques et de télécommunications d'une façon qui contrevient aux droits d'auteurs, telles que la distribution de logiciels, jeux, fichiers multimédias ou autres formats sans la permission des auteurs ;

Installation de logiciels

L'utilisation, l'installation et / ou le téléchargement de logiciels de jeux, de conversation électronique en ligne ou tout autre logiciel sur le Système d'Information de la collectivité (Sauf après approbation du service informatique) ;

Accès à distance

L'utilisation, l'installation et / ou le téléchargement de logiciels permettant d'accéder à distance aux équipements, aux ressources informatiques et de télécommunications et /ou au réseau doivent être réservés uniquement à un usage interne et interdit pour toute personne extérieure à la collectivité ;

Hygiène des salles informatiques

Manger, boire et / ou fumer dans les salles informatiques.

Annexe 3 – Mots de Passe

Ne le divulguez à personne, ne le mettez pas en mémoire dans votre ordinateur et ne l'écrivez nulle part.

En ayant accès à votre mot de passe, un individu pourrait avoir accès à vos données confidentielles et effectuer des transactions frauduleuses en votre nom. C'est ce qu'on appelle le vol d'identité.

Un mot de passe complexe :

- Comprend au moins douze caractères ;
- Ne contient ni votre nom d'utilisateur, ni votre vrai nom, ni le nom de la collectivité ;
- Ne contient pas de mot entier ;
- Est complètement différent des mots de passe précédents ;
- Contient des caractères provenant de chacune des quatre catégories suivantes :

Catégorie de caractère	Exemple
Lettres majuscules	A, B, C
Lettres minuscules	a, b, c
Chiffres	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Caractères spéciaux	` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /

La méthode suivante vous permet de créer un mot de passe à la fois difficile à pirater et facile à retenir :

- Choisissez une phrase ou un titre de chanson.
- Prenez les deux premiers caractères de chacun des mots.
- Alternez majuscule et minuscule et remplacez certaines lettres par des caractères spéciaux ou des chiffres.

Exemple : « Je me souviens du mot de passe » devient JeMe5oDuMoDeP@ (« S » est remplacé par le chiffre « 5 » et « a » par le caractère « @ »).

Évitez :

- Les mots de passe faciles à taper, tels que 123abc ou 99999 : ils sont trop faciles à déduire ou à apercevoir par-dessus votre épaule lors de leur saisie ;
- Un mot de passe identique à votre code d'accès. Les fraudeurs tentent souvent cette option en premier ;
- Un mot de passe unique pour tous vos accès : si votre mot de passe est découvert, le fraudeur pourrait accéder aux autres systèmes ou sites transactionnels que vous utilisez.

Calculer la « robustesse » d'un mot de passe

Par abus de langage, on parle souvent d'un mot de passe « robuste » pour désigner sa capacité à résister à une énumération de tous les mots de passe possibles.

https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

Gestionnaire de mots de passe :

Il est recommandé d'utiliser un gestionnaire de mots de passe de type KEEPASS
https://cyber.gouv.fr/produits-certifies/keepass-version-210-portable