Envoyé en préfecture le 13/06/2025
Reçu en préfecture le 13/06/2025
Publié le 13/06/2025
ID : 062-246200638-20250612-D_2025_140-AR

SIVOM communauté du Béthunois
Acteur de votre quotidien

Décision n°D_2025_140

INFORMATIQUE

ADOPTION DE LA CHARTE INFORMATIQUE

Nous, Pierre-Emmanuel GIBSON, Président du SIVOM de la Communauté du Béthunois,

Vu le Code Général des Collectivités Territoriales et notamment l'article L 5211-10,

Vu la délibération n° 1-06 du Comité syndical en date du 16 juillet 2020 modifiée les 26 mars 2021 et 22 juin 2022, autorisant le Président, notamment à approuver ou modifier tout document permettant de réglementer les modalités d'exercice des compétences du SIVOM de la Communauté du Béthunois (règlements de service, …),

Considérant que le développement des technologies de l'information et de la communication conduit les agents du SIVOM de la Communauté du Béthunois à utiliser dans leur travail quotidien l'outil informatique, les réseaux et les services de communication numériques pour l'exécution de leurs missions ; que cette utilisation peut comporter un certain nombre de risques à la fois techniques mais également juridiques pouvant engager la responsabilité de la collectivité et de ses agents,

Considérant qu'il appartient au SIVOM de la Communauté du Béthunois, en qualité d'institution publique et d'employeur, de promouvoir une utilisation loyale, responsable et sécurisée du système d'information, dans le respect de la réglementation en vigueur notamment en matière de protection des données,

Considérant la volonté du SIVOM de la Communauté du Béthunois de maintenir l'intégrité de son système d'information et de garantir un niveau de performance satisfaisant à tous les utilisateurs des ressources informatiques,

Considérant par conséquent qu'il convient d'adopter une charte informatique posant les règles relatives à l'utilisation de ces ressources au sein du SIVOM de la Communauté du Béthunois,

Considérant l'avis favorable du Comité Social Territorial en date du 12 juin 2025,

DECIDONS :

Article 1er : D'adopter la charte informatique, dès sa publication, telle qu'annexée à la présente décision.

Article 2 : Cette charte sera communiquée à tous les agents de l'établissement afin qu'ils en prennent connaissance et s'engagent à la respecter.

Envoyé en préfecture le 13/06/2025
Reçu en préfecture le 13/06/2025
Publié le 13/06/2025
ID : 062-246200638-20250612-D_2025_140-AR

Article 3 : Madame la Directrice Générale des Services est chargée de prendre toutes mesures nécessaires en vue de l'exécution de la présente décision.

Béthune,

Pierre Emmanuel Gibson
Président du SIVOM de la Communaute du Bethunois
13 juin 2025

Cette décision peut faire l'objet d'un recours gracieux par saisine de son auteur ou d'un recours contentieux devant le tribunal administratif de Lille, dans un délai de deux mois à compter de sa publication.

Envoyé en préfecture le 13/06/2025
Reçu en préfecture le 13/06/2025
Publié le
ID : 062-246200638-20250612-D_2025_140-AR

CHARTE INFORMATIQUE

La présente charte a pour objet de définir les règles d'utilisation des ressources informatiques mises à disposition des agents du SIVOM de la Communauté du Béthunois. Elle vise à garantir la sécurité du système d'information, à prévenir les abus et à assurer une utilisation conforme aux exigences légales et aux besoins professionnels. Elle s'inscrit dans le cadre des réglementations en vigueur, notamment le Règlement Général sur la Protection des Données (RGPD) et la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

SIVOM de la Communauté du Béthunois

660 rue de Lille - 62400 BETHUNE

Envoyé en préfecture le 13/06/2025
Reçu en préfecture le 13/06/2025
Publié le
ID : 062-246200638-20250612-D_2025_140-AR

1. Champ d'application

La présente charte s'applique à l'ensemble des agents du SIVOM de la Communauté du Béthunois tous statuts confondus, et plus généralement à l'ensemble des personnes, permanentes ou temporaires, utilisant les moyens informatiques de l'entité ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir du réseau administré par l'entité. Elle couvre :

- L'utilisation des équipements informatiques (ordinateurs, tablettes, téléphones professionnels, imprimantes, etc.).
- L'accès aux réseaux internes et à Internet.
- L'usage des logiciels métiers et outils bureautiques.
- L'utilisation de la messagerie électronique et des outils de communication.
- La gestion des données et documents numériques.

2. Principes généraux

- L'utilisation des ressources informatiques doit être conforme aux missions de la collectivité et s'inscrire dans un cadre professionnel.
- Toute utilisation à des fins personnelles doit rester occasionnelle, raisonnable et ne pas nuire au bon fonctionnement des services.
- L'accès aux ressources informatiques implique l'acceptation pleine et entière des règles définies dans cette charte.
- Chaque utilisateur est responsable de l'utilisation qui est faite de son accès et des actions effectuées sous son identité numérique.
- Toute violation des règles de sécurité peut entraîner des sanctions disciplinaires.

3. Accès aux ressources informatiques

- L'attribution des accès informatiques est strictement encadrée et basée sur les fonctions et responsabilités de chaque utilisateur.
- Les comptes utilisateurs sont strictement personnels et ne doivent en aucun cas être partagés.
- En cas d'absence momentanée, les utilisateurs doivent verrouiller leur session.
- Toute absence prolongée doit être signalée afin de désactiver temporairement les accès si nécessaire.
- Toute connexion suspecte ou toute tentative d'accès non autorisée doit être signalée immédiatement au service informatique.
- Le matériel personnel (clés USB, disques durs externes, smartphones, etc.) ne peut être connecté au réseau informatique de la collectivité sans validation préalable du service informatique.
- Les matériels doivent être éteints à chaque fin de poste.

Envoyé en préfecture le 13/06/2025
Reçu en préfecture le 13/06/2025
Publié le
ID : 062-246200638-20250612-D_2025_140-AR

4. Sécurité du système d'information

- **Mots de passe** : Ils doivent respecter la politique de robustesse en vigueur dans la collectivité. Les mots de passe ne se notent pas et ne se transmettent pas.
- **Logiciels** : Les utilisateurs ne doivent pas installer, télécharger ou utiliser sur le matériel des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, et sans autorisation du service informatique.
- **Mises à jour** : Les mises à jour des systèmes et logiciels doivent être appliquées régulièrement pour garantir la sécurité.
- **Utilisation des supports amovibles** : Les clés USB et disques durs externes doivent être scannés avec un antivirus avant utilisation et leur usage doit être limité aux besoins strictement professionnels.
- **Accès distant** : Toute connexion à distance doit s'effectuer via un VPN sécurisé mis en place par la collectivité.
- **Sauvegarde des données** : Les utilisateurs doivent enregistrer leurs documents sur les serveurs sécurisés de la collectivité et non sur des supports locaux.

5. Utilisation d'Internet

Le SIVOM de la Communauté du Béthunois est fournisseur d'accès internet (FAI) lorsqu'il fournit un accès à internet quel que soit le biais (filaire ou wifi). La navigation sur internet s'effectue avec les adresses IP publiques du SIVOM, engageant ainsi la responsabilité de son Président en cas d'usage délictueux.

De ce fait, le SIVOM est tenu au respect d'un certain nombre d'obligations parmi lesquelles :

- ✓ L'identification et la journalisation des informations de connexion et de navigation (durée, sites visités, téléchargements) ainsi que leur conservation sur une année.
- ✓ Le filtrage de la navigation, par le blocage de sites dont la consultation est illicite et punie par la loi.
- ✓ Le constat de toute utilisation illégale pourra donner lieu, après décision actée de l'autorité administrative ou judiciaire, à la suppression des accès et/ou à des sanctions disciplinaires.

- La navigation sur Internet est autorisée uniquement pour des besoins professionnels. Néanmoins, il est toléré pour un usage modéré d'accéder à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel.
- L'accès à des sites à caractère pornographique, incitant à la haine, frauduleux ou illégaux est interdit.
- L'utilisation de forums de discussion est autorisée pour un usage professionnel sous réserve du respect des obligations des agents publics (réserve, neutralité, etc.).
- Le téléchargement, en tout ou partie, de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.) est strictement interdit.
- Le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet est interdit.

Cas des réseaux sociaux

- La Direction Générale des Services détermine les agents habilités à communiquer sur les réseaux sociaux au nom et pour le compte de l'Institution.
- L'usage des réseaux sociaux à des fins professionnelles doit être encadré et validé par la direction générale.
- La distinction entre l'utilisation professionnelle et l'utilisation personnelle est recommandée (création de deux profils)

6. Utilisation de la messagerie électronique

L'adresse de messagerie qui a été remise à l'agent demeure à usage professionnel exclusivement et ne doit être communiquée ou utilisée sur des sites sans rapport avec les missions de l'agent (mailings et différents services privés, etc.).

Un usage raisonnable dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que l'utilisation du courrier électronique soit conforme aux dispositions de la présente charte et au droit informatique, qu'elle n'affecte pas le trafic normal des messages professionnels et qu'elle ne gêne en rien les activités du SIVOM de la Communauté du Béthunois.

- L'envoi de courriels doit respecter les règles de courtoisie et de confidentialité.
- L'envoi de pièces jointes volumineuses doit être limité ; des solutions de partage sécurisées sont à privilégier. L'utilisateur n'aura pas recours à des services en ligne nécessitant le dépôt de données sur des serveurs tiers. A des fins de sécurité et de confidentialité, les services d'envois de fichiers volumineux tels que WeTransfer sont à proscrire. Le SIVOM de la Communauté du Béthunois a mis en place un service équivalent permettant d'envoyer et de recevoir des fichiers de grande capacité. Cette plateforme est propre au SIVOM et répond aux principes de sécurité liés au transfert de la donnée.
- L'ouverture de pièces jointes et de liens provenant d'expéditeurs inconnus doit être effectuée avec prudence. L'utilisateur ne doit pas ouvrir des messages dont l'origine, l'objet ou le contenu est douteux, ou exécuter les pièces jointes suspectes. En cas de réception d'un tel message, il avertit le service informatique et ne prend pas d'initiative sans la validation de celui-ci. Pour limiter les risques et sensibiliser les utilisateurs à la menace que représente le « Phishing », les utilisateurs sont tenus de suivre le programme de sensibilisation relatif à cette menace.

Cas des messages personnels.

Les messages personnels doivent être marqués « PERSONNEL » ou « PRIVÉ » et être stockés dans un répertoire portant le même nom. Le SIVOM n'assume aucune responsabilité quant à la sauvegarde des données privées des agents.

Cas des absences.

L'utilisateur devra utiliser le gestionnaire d'absence pour la période durant laquelle il ne pourra prendre connaissance des messages. Il fournira notamment l'adresse mail à contacter pour l'ensemble de la durée concernée.

Dans le cadre de la continuité de service, la collectivité se réserve la possibilité, en cas d'absence prolongée ou imprévue d'un collaborateur (congés, arrêt maladie, mission extérieure, etc.), de

permettre à la hiérarchie ou à toute personne habilitée d'accéder aux outils informatiques professionnels (messagerie électronique, fichiers, agenda, etc.) du collaborateur concerné.

Cet accès a pour unique objectif d'assurer la bonne continuité de l'activité et est strictement encadré. Il est exercé dans le respect du secret des correspondances et de la vie privée. À ce titre :

- Seuls les courriels et fichiers professionnels peuvent être consultés.
- En cas de doute sur la nature privée ou professionnelle d'un courriel ou fichier, il ne sera pas ouvert sans l'accord du collaborateur ou, à défaut, selon une procédure encadrée (présence d'un tiers, information du Délégué à la Protection des Données, etc.).
- Le collaborateur est invité à identifier clairement les fichiers ou messages à caractère personnel (par exemple en utilisant un dossier ou une mention "Personnel").

Toute action d'accès aura été validée préalablement par la Direction Générale. Cette action sera tracée et le collaborateur sera informé, a posteriori, de l'accès à ses données.

7. Protection des données

- Toute collecte, stockage ou transmission de données personnelles doit être réalisée en conformité avec le RGPD.
- L'accès aux informations sensibles est limité aux seuls agents habilités.
- Les postes de travail doivent être verrouillés en cas d'absence prolongée.
- Les sauvegardes des données critiques sont réalisées régulièrement par le service informatique.
- La suppression définitive de données sensibles doit respecter les protocoles en vigueur (effacement sécurisé, destruction physique de supports, etc.).
- L'usage d'outils de stockage cloud non validés par la collectivité est interdit.

8. Télétravail et accès à distance

- Le télétravail est autorisé sous réserve d'une validation préalable par la hiérarchie et dans le cadre défini par guide interne de la collectivité. (cf Guide du télétravail disponible dans la Base Documentaire)
- L'accès aux ressources informatiques à distance doit obligatoirement s'effectuer via un VPN sécurisé mis en place par la collectivité.
- Les agents en télétravail doivent utiliser exclusivement le matériel fourni par la collectivité (PC, téléphone, etc.).
- L'usage du Wi-Fi domestique doit être sécurisé (mot de passe robuste, chiffrement WPA2/WPA3).
- Toute activité professionnelle en télétravail doit respecter les mêmes règles de confidentialité et de sécurité que sur site.
- Les documents confidentiels ne doivent pas être stockés localement sur les équipements personnels ou partagés.
- Tout incident de sécurité (perte ou vol de matériel, tentative d'accès suspecte, etc.) doit être signalé immédiatement au service informatique.

9. Mise à disposition des matériels et responsabilité des utilisateurs

- Tout matériel informatique (ordinateur, téléphone, tablette, etc.) est mis à disposition des agents pour un usage strictement professionnel. Ils restent la propriété du SIVOM de la Communauté du Béthunois.
- Chaque agent est responsable du matériel qui lui est confié et doit en prendre soin.
- Il est obligatoire de protéger son téléphone mobile ou sa tablette par un système de verrouillage (mot de passe, code PIN, schéma de déverrouillage)
- L'utilisateur s'interdit de prêter les outils informatiques, notamment les équipements portables, mis à sa disposition et ce, dans le cadre professionnel comme personnel.
- En cas de perte, vol ou détérioration du matériel, l'agent doit en informer immédiatement le service informatique.
- Durant les déplacements, l'utilisateur conserve la charge et la responsabilité du matériel mis à disposition. Dans le cas de déplacements avec un véhicule quel qu'il soit, le matériel ne devra pas être laissé dans le véhicule. Les variations de température, l'humidité extérieure, les risques de vols, sont autant de risques pouvant engendrer des défaillances du/des matériel(s).
- En cas de cessation de fonction ou de mutation, l'agent doit restituer l'ensemble du matériel mis à disposition en bon état.

10. Départ d'un agent

- En cas de départ d'un agent (démission, mutation, retraite, fin de contrat, etc.), ses autorisations seront retirées immédiatement par le SIVOM de la Communauté du Béthunois. Toute autorisation (compte, l'adresse électronique nominative et l'ensemble des accès aux systèmes, réseaux (dossiers partagés) et applications ou progiciels) prend fin lors de la cessation, même provisoire, de l'activité professionnelle.
- L'agent devra supprimer toute donnée privée ou personnelle sur tout support (poste de travail, tablette, téléphone, supports amovibles, etc.), y compris sur sa messagerie avant de rendre son matériel.
- Avant son départ, l'agent mettra à disposition de son supérieur les éventuelles données professionnelles que l'utilisateur est le seul à détenir. Le supérieur hiérarchique évaluera la pertinence de ce qui doit être récupéré et de ce qui peut être détruit.
- Lors de son départ, l'utilisateur doit remettre l'ensemble des moyens informatiques et de communication mis à sa disposition pour l'exercice de son activité professionnelle à son responsable hiérarchique.

11. Réglementation

Il est rappelé que toute personne sur le sol français doit respecter la législation française en particulier dans le domaine de la sécurité informatique :

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée (cnil.fr).
- Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain.
  (articles 323-1 à 323-7 du Code pénal - Livre III - Titre II - Chapitre III), (legifrance.gouv.fr)

- Loi n° 94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels (legifrance.gouv.fr)
- Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme.
- Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (« LCEN »).
- Règlement européen de protection des données (« RGPD ») du 27 avril 2016 (eurlex.europa.eu).
- Règlement (UE) N°910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur («eIDAS ») du 23 juillet 2014 (eur-lex.europa.eu).
- Législation applicable en matière de sécurité de l'information (cyber.gouv.fr.)

12. Sanctions et responsabilité

- Toute infraction aux règles établies dans cette charte peut entraîner la suspension d'accès aux ressources informatiques, des sanctions disciplinaires, voire des poursuites judiciaires en cas de faute grave.
- La collectivité se réserve le droit de contrôler, dans le respect des dispositions légales, l'utilisation des ressources informatiques afin d'assurer la sécurité et le bon fonctionnement du système d'information.
- En cas de manquement grave à la sécurité, la collectivité pourra engager la responsabilité individuelle de l'agent concerné.
- L'usager s'engage à signaler toute anomalie ou incident de sécurité au service informatique.

13. Acceptation et mise en application

Cette charte entre en vigueur à compter de sa validation par l'autorité compétente. Tout utilisateur des ressources informatiques doit signer un engagement de respect des règles définies.

Je soussigné :

Nom : …….. Prénom : ……..

Service : …….. Fonction : …….. ,

Utilisateur / utilisatrice des moyens informatiques et réseaux de la collectivité, déclare avoir pris connaissance de la présente charte et m'engage à la respecter.

Fait à …….. , le ……..

Signature……..