Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

VILLE DE SAINT-LAURENT-BLANGY
www.saint-laurent-blangy.fr

EXTRAIT DU REGISTRE

DES DELIBERATIONS DU CONSEIL MUNICIPAL

SÉANCE du 15 décembre 2025

Délibération N° 15/12/2025 2-1

ADOPTION D'UNE NOUVELLE CHARTE D'USAGE ET DE SECURITE POUR LES UTILISATEURS DU SYSTEME D'INFORMATION DU SERVICE COMMUN INGENIEURIE INFORMATIQUE, TELECOMMUNICATIONS ET USAGES NUMERIQUES

L'an deux mille vingt-cinq, le 15 décembre à 18 heures, le Conseil Municipal s'est réuni au lieu ordinaire de ses séances sous la présidence de Monsieur Nicolas DESFACHELLE en suite de convocation en date du 9 décembre 2025 dont un exemplaire a été affiché à la porte de la Mairie.

Étaient présents : Nicolas DESFACHELLE, Christophe LOURME, Laurence FACHAUX-CAVROS, Fabrice CAPRON, Béatrice WOZNIAK, Nicolas KUSMIEREK, Lise-Marie MARTEL, Philippe MERCIER, Pierre-Marie SOUILLARD, Nathalie CARTIGNY, Marc LABUR, Fatima ATTINI, Alain STEUX, Sandrine NOWAK, Christophe COUPARD, Jean-Fabrice PINGUIN, Florence CAUDRON, Corinne MERCIER, Aurélie LITTAYE, Angélique DELMEIREN, Jean-Christophe CAMBIER, Laura OLENDER

Étaient absents excusés :

Mme Karine GOUBE qui a donné procuration à Mme Laurence FACHAUX-CAVROS
M. Frédéric HOUPLAIN qui a donné procuration à M. Philippe MERCIER
M. Serge BRUNEAU
Mme Fabienne CAMUS qui a donné procuration à Mme Béatrice WOZNIAK
Mme Maggy JANSSOONE
M. Lucas CHASSAGNE

Était absent :

M. Thierry PLOUVIEZ

Mme Béatrice WOZNIAK est élue Secrétaire.

La séance ouverte, M. le Président donne lecture du rapport ci-après :

« Monsieur le Maire donne lecture du rapport suivant :

Mesdames, Messieurs,

Vu l'avis du Comité Social Territorial en date du 18/11/2025 ;

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

Considérant le développement et l'utilisation croissante des outils informatiques et numériques au sein des services de la Communauté Urbaine d'Arras et des communes adhérentes au service commun « Informatique, Télécommunication et Usages Numériques » constitué à compter du 1er janvier 2025, à savoir les communes d'Arras, Saint-Laurent-Blangy et Saint-Nicolas-lez-Arras ;

Considérant la nécessité de garantir la sécurité des systèmes d'information, des données et le respect des obligations légales en matière de protection des données personnelles ;

Considérant qu'il est essentiel d'adopter une charte informatique permettant de définir clairement les droits, devoirs et responsabilités des utilisateurs communautaires concernant l'usage des équipements, réseaux et logiciels mis à leur disposition ;

Considérant que cette charte informatique vise à encadrer l'utilisation des ressources informatiques de la Communauté Urbaine d'Arras afin d'assurer la sécurité et confidentialité des données, le respect des règles légales en matière de propriété intellectuelle et le bon fonctionnement du service commun « Informatique, Télécommunication et Usages Numériques » constitué à compter du 1er janvier 2025 entre la Communauté Urbaine d'Arras et les communes d'Arras, Saint-Laurent-Blangy et Saint-Nicolas-lez-Arras ;

La charte informatique annexée à la présente délibération entrera en vigueur dès sa publication et sera applicable à l'ensemble des utilisateurs, permanents ou temporaires, ainsi qu'aux prestataires externes travaillant au sein des locaux ou utilisant les équipements informatiques de la collectivité ;

La charte informatique définit les principes d'utilisation concernant :

- L'utilisation responsable et sécurisée des outils numériques et équipements informatiques ;
- La protection des données personnelles et des informations sensibles traitées par les services communautaires ;
- La prévention des risques liés aux cyberattaques et aux accès non autorisés aux systèmes d'information ;
- Le respect des droits de propriété intellectuelle et la bonne utilisation des licences logicielles.

La charte informatique sera annexée au règlement intérieur de la collectivité, afin de garantir son application et de rappeler son caractère obligatoire pour tous les utilisateurs.

Il est prévu que des actions de sensibilisation soient mises en place pour informer les utilisateurs des bonnes pratiques et des règles à respecter en matière de sécurité informatique, de protection des données, et d'utilisation des outils numériques.

Un comité de suivi sera chargé d'assurer la bonne application de la charte informatique. Ce comité proposera, si nécessaire, des mises à jour régulières de la charte afin de l'adapter aux évolutions technologiques et réglementaires.

Une commission de recueil des signalements sera créée au sein de la commune et sera composée d'un élu du Conseil Municipal désigné par Monsieur le Maire, d'un représentant de la direction générale, d'un représentant du service des ressources humaines, d'un représentant du personnel et d'un représentant du service de sécurité informatique du service commun.

Toute infraction aux règles définies par la charte informatique pourra entraîner des sanctions disciplinaires conformément aux dispositions du règlement intérieur de la collectivité et aux textes en vigueur.

La charte informatique sera communiquée à tous les utilisateurs. Des exemplaires imprimés seront également mis à disposition dans chaque service.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

Compte tenu de ce qui précède, il vous est aujourd'hui proposé de bien vouloir :

- Adopter une nouvelle charte d'usage et de sécurité pour les utilisateurs du système d'information du service commun « Informatique, Télécommunication et Usages Numériques » constitué à compter du 1er janvier 2025 entre la Communauté Urbaine d'Arras et les communes d'Arras, Saint-Laurent-Blangy et Saint-Nicolas-lez-Arras ;
- Approuver les termes de ladite Charte ;
- Autoriser Monsieur le Maire à désigner Madame Sandrine NOWAK pour siéger au sein de la commission de recueil des signalements ;
- Autoriser Monsieur le Maire à signer ladite charte ainsi que toute pièce relative à la mise en œuvre de la présente délibération.

« La présente décision est susceptible de faire l'objet d'un recours contentieux devant le Tribunal administratif de Lille dans les deux mois à compter de sa publication.
Elle est également susceptible de faire l'objet d'un recours gracieux dans le même délai. Un recours contentieux peut ensuite être formé auprès du Tribunal administratif de Lille dans le délai de deux mois suivant le rejet explicite ou implicite du recours gracieux »

Le rapport est adopté à l'unanimité.

Nicolas DESFACHELLE
Maire,

MAIRIE DE SAINT-LAURENT-BLANGY (Pas-de-Calais)

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

CHARTE D'USAGE ET DE SÉCURITÉ POUR LES UTILISATEURS DU SYSTÈME D'INFORMATION DU SERVICE COMMUN « INFORMATIQUE, TELECOMMUNICATIONS ET USAGES NUMERIQUES »

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

1. CHAMP D'APPLICATION

Cette charte concerne toutes les collectivités qui ont signé une convention cadre avec le système d'information mutualisé, mise en œuvre et maintenu par la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques de la Communauté Urbaines d'Arras Elle s'applique à tous les utilisateurs de ces systèmes, qu'ils soient agents de la collectivité, prestataires externes, ou toute autre personne ayant accès aux ressources numériques. Chaque utilisateur est responsable de la compréhension et du respect de cette charte. Parmi les utilisateurs on trouvera notamment :

- Les élus,
- Les agents territoriaux (titulaires ou contractuels, stagiaires),
- Les vacataires,
- Les stagiaires, apprentis ou équivalents,
- Les intérimaires,
- Les employés de sociétés prestataires,

A noter que les visiteurs externes non couverts par une relations contractuelles avec la collectivité ne doivent pouvoir accéder qu'aux ressources mise à disposition à cette effet (Wi-Fi invité notamment) et ceci dans le cadre de l'utilisation prévue à cet effet.

2. GLOSSAIRE

1. **CATI :** Centre d'assistance technique informatique, chargé de fournir un support aux utilisateurs pour les questions techniques relatives au système d'information.
2. **Chiffrement des Données :** Méthode de protection des données rendant leur lecture impossible sans clé d'accès, assurant la confidentialité lors du stockage et du transfert des informations.
3. **Collectivité :** Entités signataires d'une convention cadre pour l'utilisation du système d'information mutualisé. Elle regroupe la Communauté Urbaine d'Arras et les communes d'Arras, Saint-Laurent-Blangy, et Saint-Nicolas-lez-Arras.
4. **Commission de Recueil des Signalements :** Instance composée de représentants qualifiés et indépendants, en charge de la réception et de l'examen des signalements d'infractions ou comportements inappropriés (harcèlement, discrimination, etc.).
5. **Données :** Ensemble des informations traitées, stockées et échangées, pouvant être structurées (bases de données) ou non structurées (documents, courriels, fichiers multimédias).
6. **Données à Caractère Personnel :** Informations permettant d'identifier une personne physique, telles que le nom, un identifiant unique, des données de localisation, etc., conformément au RGPD.
7. **DPO (Data Protection Officer) :** Délégué à la Protection des Données, chargé de veiller au respect des lois sur la protection des données personnelles et du RGPD.
8. **Droit à la Déconnexion :** Droit des utilisateurs de ne pas être sollicités en dehors de leurs heures de travail définies, visant à respecter l'équilibre entre vie privée et vie professionnelle.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

9. **Enquête Administrative** : Investigation interne initiée par la collectivité pour examiner les infractions aux règles de la charte ou d'autres comportements répréhensibles.

10. **Habilitations** : Droits d'accès spécifiques accordés aux utilisateurs selon leur rôle et leurs responsabilités. Ces droits sont révoqués en cas de départ ou d'absence prolongée.

11. **Identifiants de Connexion** : Combinaison d'un nom d'utilisateur et d'un mot de passe qui assure l'accès sécurisé aux systèmes d'information.

12. **Intelligence Artificielle (IA)** : Technologie simule des traitements de l'intelligence humaine. Dans le contexte de la collectivité, elle est utilisée de manière éthique, selon des principes de transparence, de sécurité et de durabilité.

13. **Messagerie Professionnelle** : Service de courrier électronique fourni par la collectivité pour un usage strictement professionnel, accessible pour assurer la continuité du service en cas d'absence prolongée de l'utilisateur.

14. **Nomadisme Numérique** : Pratique permettant aux utilisateurs de travailler à distance ou en déplacement, exigeant des mesures de sécurité renforcées pour protéger les informations sensibles.

15. **Plan de Continuité d'Activité (PCA)** : Ensemble de mesures visant à garantir la continuité des services et des opérations en cas d'incident majeur ou de panne.

16. **Règlement Général sur la Protection des Données (RGPD)** : Réglementation européenne visant à protéger les données personnelles et à réguler leur traitement.

17. **Ressources Partagées** : Infrastructures et services (serveurs de fichiers, messageries partagées, intranet) permettant aux utilisateurs de stocker et d'échanger des informations professionnelles.

18. **Réseaux de Communication** : Ensemble des technologies et dispositifs permettant de relier entre eux les composants du système d'information (réseaux locaux, étendus, VPN, etc.).

19. **Sécurité du Système d'Information (SSI)** : Mesures mises en œuvre pour garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité des informations contre les cybermenaces.

20. **Service Support** : Service chargé de l'assistance technique aux utilisateurs du système d'information.

21. **Sous-Traitants et Prestataires** : Fournisseurs externes impliqués dans la gestion, l'hébergement, ou la maintenance des composants du SI, ou encore dans la fourniture de solutions logicielles ou matérielles.

22. **Système d'Information (SI)** : Ensemble structuré des infrastructures matérielles, logiciels, réseaux, et procédures de gestion permettant le traitement, le stockage, la diffusion et la sécurité des informations.

23. **Télétravail et Mobilité** : Modalités de travail en dehors des locaux de la collectivité, demandant des pratiques de sécurité renforcées pour garantir la protection des données.

24. **Traçabilité** : Suivi et enregistrement des activités des utilisateurs dans le SI, à des fins de sécurité, de maintenance et de conformité.

25. **Utilisateur** : Toute personne ayant accès aux ressources numériques du SI (agents territoriaux, élus, prestataires externes, stagiaires, etc.), responsable du respect des règles d'accès et de sécurité.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

26. **VPN (Virtual Private Network)** : Technologie qui permet de créer une connexion sécurisée à un réseau via Internet, utilisée pour garantir la confidentialité des échanges de données, en particulier en situation de télétravail.

3. COMPOSITION DU SYSTEME D'INFORMATION

Le Système d'Information (SI) est l'ensemble structuré de ressources permettant de collecter, traiter, stocker, diffuser et sécuriser des informations au sein d'une organisation. Cela comprend les infrastructures matérielles, les logiciels, les réseaux de communication, les données et la sécurité du SI.

- Infrastructures matérielles (Hardware) : Ensemble des équipements physiques tels que les serveurs, postes de travail, périphériques réseau (routeurs, switches), dispositifs de stockage (NAS, SAN) et équipements de sécurité (pare-feu, systèmes de détection d'intrusion).

- Logiciels et applications (Software) : Programmes et applications métiers, systèmes d'exploitation, logiciels de gestion, outils de communication et de collaboration, ainsi que les systèmes de gestion de bases de données.

- Réseaux de communication : Ensemble des dispositifs permettant de relier entre eux les composants du système d'information, incluant les réseaux locaux (LAN), réseaux étendus (WAN), connexions Internet, VPN, et autres technologies facilitant les échanges de données.

- Données : L'ensemble des informations traitées, stockées et échangées au sein de l'organisation. Les données peuvent être structurées (bases de données) ou non structurées (documents, courriels, fichiers multimédias).

- Sécurité du Système d'Information (SSI) : Mesures et dispositifs mis en place pour assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, ainsi que la protection contre les cybermenaces. Cela inclut la gestion des identités et des accès, les protocoles de chiffrement, les sauvegardes et les plans de continuité d'activité (PCA).

- Ressources humaines : Les utilisateurs du SI, incluant les administrateurs système, les développeurs, le personnel informatique, ainsi que l'ensemble des employés ayant accès aux outils et données de l'organisation.

- Procédures et processus : Ensemble des règles, méthodes et procédures qui encadrent l'utilisation, la gestion et la maintenance du SI. Cela inclut les processus de gestion du changement, de traitement des incidents, et de gestion des risques.

- Sous-traitants et prestataires : Les fournisseurs de services tiers qui peuvent être impliqués dans la gestion, l'hébergement, ou la maintenance des composants du SI, ainsi que dans la fourniture de solutions logicielles ou matérielles.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

4. PRINCIPES GENERAUX

Cette charte a pour objectif de définir les conditions d'utilisation des moyens informatiques et des outils numériques mis à disposition des utilisateurs du service commun.

Elle vise à assurer la sécurité des systèmes d'information, la protection des données et la responsabilité partagée de tous les utilisateurs.

Le respect de cette charte est une obligation professionnelle et elle est intégrée au règlement intérieur de chacune des collectivités ou groupement de collectivités concernés par le service commun.

Le non-respect de la charte implique des sanctions telles que définies dans les règlements intérieurs.

Les règles de la présente charte s'appliquent quelle que soit le statut de l'utilisateur:

- Dans les locaux de chacune des collectivités ou groupement de collectivités concernés par le service commun
- En situation de mobilité
- En situation de télétravail.

4.1. OBLIGATIONS DES UTILISATEURS DES OUTILS INFORMATIQUES

Dans l'utilisation des outils informatiques, chaque utilisateur doit agir avec impartialité, intégrité et probité. Il/elle est également tenu(e) à l'obligation de neutralité et au respect du principe de laïcité.

À ce titre, l'utilisateur doit s'abstenir de manifester ses opinions personnelles dans l'exercice de ses missions. Il/elle traite toutes les personnes de manière égale et respecte leur liberté de conscience ainsi que leur dignité.

Les écrits ne doivent contenir aucune intention violente ou avoir un caractère de discrimination, de harcèlement moral ou sexuel, ou d'agissements sexistes. Si un utilisateur s'estime victime de tels agissements, il/elle a la possibilité de le signaler à la Commission de Recueil des Signalements.

Il convient de faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont les utilisateurs ont connaissance dans le cadre de l'utilisation du Système d'Information.

La sécurité du Système d'Information doit être une préoccupation permanente ; par ses usages, l'utilisateur est le premier acteur de la sécurité de l'information.

La Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques est garante du bon fonctionnement et de la sécurité du Système d'Information. Les utilisateurs doivent se conformer à ses directives en toutes circonstances.

4.2. COMMISSION DE RECUEIL DES SIGNALEMENTS

La commission est composée de représentants des ressources humaines, de représentants des

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

employés, ainsi que de membres indépendants qualifiés, choisis pour garantir une prise en charge impartiale et équitable des signalements.

La commission a pour mission de :

- Recevoir et examiner les signalements relatifs aux comportements inappropriés, y compris le harcèlement, la discrimination, les agissements sexistes, et les violations du principe de neutralité.
- Mener des enquêtes approfondies sur les faits rapportés.
- Proposer des actions correctives ou préventives en conformité avec la législation en vigueur et les politiques internes.

Les utilisateurs peuvent saisir la commission via plusieurs canaux :

- En envoyant un courriel à une adresse dédiée.
- En utilisant un formulaire sécurisé disponible sur l'intranet.
- En déposant un signalement anonyme via un canal sécurisé prévu à cet effet. La confidentialité des signalements est garantie pour protéger l'identité des plaignants et des personnes impliquées.

Après avoir étudié les faits, la commission :

1. Procède à un vote collégial pour statuer sur la situation.
2. Communique la décision aux parties concernées, accompagnée des mesures à mettre en œuvre, si nécessaire (sanctions, sensibilisation, etc.).
3. Les décisions sont prises dans le respect de la législation et des procédures internes afin de garantir équité et transparence.

4.3. PARCOURS CYBER A L'ARRIVEE D'UN UTILISATEUR

Lors de l'arrivée d'un nouvel utilisateur au sein de l'une quelconque des collectivités ou groupement de collectivités concernés par le service commun, il est obligatoire que celui-ci suive un parcours de sensibilisation à la cybersécurité avant d'être autorisé à utiliser les systèmes d'information de la collectivité ou du groupement de collectivités concerné(e).

Ce parcours vise à informer l'utilisateur des bonnes pratiques en matière de sécurité numérique, des risques liés à l'utilisation des outils informatiques et des responsabilités individuelles pour protéger les données dites sensibles. L'utilisateur devra suivre obligatoirement ce parcours et attester de sa compréhension des enjeux de sécurité avant que ses accès ne soient activés. Un questionnaire sera soumis à l'agent aux termes de la formation dont le résultat permettra d'attester de sa compréhension

Cette démarche garantit que tous les utilisateurs ont un niveau de vigilance et de compétence en cybersécurité adapté aux exigences de la collectivité ou du groupement de collectivité concerné(e).

4.4. PREVENTION DU PIRATAGE ET ACTES SIMILAIRES

Les logiciels sont des œuvres intellectuelles protégées par une législation stricte. Par conséquent, la copie privée est interdite.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

Les collectivités et le groupement de collectivités concernés par le service commun ne sauraient être tenues pour responsables de l'installation par un utilisateur d'un logiciel dont elles n'ont pas acquis les droits.

Si un utilisateur diffuse sur Internet ou récupère des images, vidéos, photos ou sons sans le consentement de leur auteur, il est en infraction.

Les données circulant sur Internet peuvent être soumises à des réglementations en termes d'utilisation ou être protégées par un droit de propriété intellectuelle. L'utilisateur est responsable de l'utilisation des données qu'il consulte et transfère, et doit notamment s'assurer qu'il dispose de toutes les autorisations nécessaires (licences d'utilisation, droits de reproduction des images, textes et sons ou vidéos).

4.5. PROTECTION DES DONNEES PERSONNELLES

4.5.1. Définitions

Le règlement général de protection des données (RGPD) du 25 mai 2018 et la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés définissent les conditions dans lesquelles des données à caractère personnel peuvent faire l'objet d'un traitement.

Selon ces textes, constitue :

- Une donnée à caractère personnel : Toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
- Un traitement : Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

À titre d'exemple, constituent des traitements de données à caractère personnel :

- Le classement et le traitement de dossiers papier de demande de subventions
- La constitution d'une base de données de contacts professionnels (mailing, liste d'entreprises).
- La mise en œuvre d'un système de billettique de transport ou de piscines.
- La géolocalisation des véhicules de collecte.
- Les enquêtes sur les ménages.
- La gestion du personnel ou de la paie.

4.5.2. Secret professionnel

Chaque utilisateur de l'une quelconque des collectivités ou du groupement de collectivités membres du service commun est tenu au secret professionnel et à la confidentialité en raison du grand nombre d'informations, notamment sensibles et nominatives, auxquelles il peut avoir accès.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

Dans le respect de la déclaration faite dans le registre des traitements constitué au titre du RGPD, chaque utilisateur s'engage à :

- Ne pas utiliser les données à caractère personnel à des fins autres que celles prévues par ses finalités ;
- 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 si cela est nécessaire à l'exécution de ses fonctions ;
- Prendre toutes les mesures conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- S'assurer, dans la limite de ses attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données.

En complément de ces engagements, chaque utilisateur doit également :

- Informer immédiatement le responsable de la sécurité informatique de toute suspicion de violation de données ou de tout incident de sécurité affectant les données personnelles ;
- Participer aux formations et mises à jour régulières en matière de sécurité des données et de protection de la vie privée ;
- Coopérer pleinement avec les audits de sécurité et les contrôles de conformité organisés par les collectivités et/ou le groupement de collectivités membres du service commun ;
- Respecter les politiques et procédures internes concernant la gestion des données personnelles, y compris les procédures de destruction sécurisée des données devenues obsolètes ou inutiles et l'archivage électronique des données.

4.5.3. Détournement de finalité des données personnelles

L'utilisation de données à caractère personnel à des fins autres que celles pour lesquelles elles ont été initialement collectées constitue un détournement de finalité, interdit par la réglementation en vigueur, notamment le Règlement Général sur la Protection des Données (RGPD), applicable depuis le 25 mai 2018.

Chaque utilisateur est donc tenu de s'assurer que les données personnelles traitées dans le cadre de ses missions sont exclusivement utilisées pour les finalités professionnelles prévues. La Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques pourra effectuer des contrôles réguliers pour s'assurer de la conformité des usages.

En cas de doute sur une finalité ou sur l'utilisation des données, l'utilisateur doit se référer au Délégué à la Protection des Données (DPO) ou au Responsable de la Sécurité des Systèmes d'Information (RSSI).

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

4.6. RISQUES EN CAS DE MANQUEMENT A CES

En cas de manquement à ces règles, l'utilisateur s'expose à des risques significatifs tels que définis dans la présente charte.

Si les dispositions des présentes règles ne sont pas respectées, les droits d'accès de l'utilisateur pourraient être restreints ou suspendus.

De plus, l'utilisateur peut être passible de sanctions disciplinaires conformément au statut général de la fonction publique. Contrairement aux salariés du secteur privé soumis au Code du travail, les fonctionnaires sont régis par des règles spécifiques, mais des poursuites civiles ou pénales peuvent également être engagées en fonction de la gravité de l'infraction, notamment en cas de violation des obligations légales.

4.7. LE DROIT A LA DECONNEXION

Chaque utilisateur dispose d'un droit à la déconnexion. Cela signifie qu'il a la possibilité de ne pas se connecter aux outils numériques de son employeur (outils collaboratifs, applications métier) et de ne pas être contacté par celui-ci en dehors de ses heures de travail (téléphone, courriel).

Ce droit s'exerce en dehors des heures correspondant à la formule de travail hebdomadaire définie avec la hiérarchie de l'utilisateur.

Si l'utilisateur estime que ce droit n'est pas respecté, il doit en premier lieu évoquer la situation avec sa hiérarchie.

Si le problème persiste, l'utilisateur peut saisir la Commission de Recueil des Signalements de sa collectivité (coordonnées en annexe).

4.8. TRAÇABILITE DES ACTIVITES ET DE L'UTILISATION INTERNET

Les collectivités et le groupement de collectivités membres du service commun assurent la traçabilité de tous les accès au système d'information et à Internet à des fins de sécurité, de statistique, de maintenance et de conformité. Cette traçabilité vise à garantir l'intégrité et la disponibilité des systèmes, ainsi qu'à suivre rigoureusement les activités des utilisateurs.

Lorsqu'un poste de travail accède au système d'information ou à Internet via le réseau de la collectivité, un VPN, ou tout autre point d'accès autorisé, les données suivantes sont enregistrées :

- L'identifiant de l'utilisateur,
- La date et l'heure de connexion,
- L'adresse IP et le nom du poste de travail ou de l'équipement utilisé,
- Les sites web visités (pour les accès Internet),
- Les applications utilisées,
- Le nombre de sessions ouvertes,
- La durée totale de l'activité de l'utilisateur,
- Le volume des données transmises (téléchargements, envois de fichiers),
- Les fichiers consultés ou modifiés,
- Les opérations effectuées sur les bases de données,

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

- Les tentatives d'accès non autorisées ou échouées,
- Les motifs d'un éventuel blocage de flux.

Ces données, conservées conformément aux exigences légales et réglementaires en vigueur, sont utilisées pour :

- Assurer la sécurité du système d'information,
- Identifier et analyser les incidents de sécurité,
- Optimiser la gestion et la performance des systèmes,
- Vérifier la conformité aux politiques de sécurité et d'utilisation,
- Faciliter les audits internes et externes,
- Analyser ou rechercher les dysfonctionnements du réseau.

Les utilisateurs sont informés que leurs activités sur le système d'information et lors de la navigation Internet sont surveillées dans le respect de la législation applicable en matière de protection des données personnelles. Toute anomalie ou activité suspecte détectée pourra donner lieu à des mesures appropriées, telles que des enquêtes internes, des sanctions disciplinaires, ou des actions correctives.

La Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques est responsable du bon fonctionnement et de la sécurité des moyens informatiques. Elle veille à ce que les règles d'usage précisées dans la présente charte soient respectées. Dans le cadre de leurs fonctions, les techniciens peuvent accéder aux informations à des fins de diagnostic ou d'administration, tout en étant tenus de préserver la confidentialité des données consultées.

En cas de manquement aux règles d'utilisation ou de risques identifiés, la Direction de l'Ingénierie Informatique se réserve le droit de :

1. Modifier ou suspendre les droits d'accès au Système d'Information,
2. Informer le responsable hiérarchique de l'utilisateur concerné.

Les données collectées ne seront utilisées qu'à des fins professionnelles et ne seront divulguées à des tiers non autorisés que dans les cas requis par la loi.

4.9. DROITS SUR LES DONNEES A CARACTERE PERSONNEL DES UTILISATEURS

Les collectivités et le groupement de collectivités concernés par le service commun, en tant qu'employeurs, collectent et traitent des données à caractère personnel concernant leurs utilisateurs.

Conformément à la réglementation en vigueur, les utilisateurs disposent, dans certaines conditions, des droits suivants sur leurs données à caractère personnel :

- Droit d'accès : Le droit d'obtenir la confirmation que des données personnelles les concernant sont traitées, et d'en obtenir une copie.
- Droit de rectification : Le droit de demander la correction des données personnelles inexactes ou incomplètes.
- Droit à l'effacement : Le droit de demander la suppression de leurs données personnelles dans certaines circonstances.
- Droit à la limitation du traitement : Le droit de demander la suspension du traitement de leurs données personnelles dans certains cas.
- Droit à la portabilité des données : Le droit de recevoir leurs données personnelles dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre responsable du traitement.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

- Droit d'opposition : Le droit de s'opposer, pour des raisons tenant à leur situation particulière, au traitement de leurs données personnelles, notamment en matière de profilage.

Pour toute information concernant les modalités d'exercice de ces droits, les utilisateurs peuvent contacter le Délégué à la Protection des Données (DPO – Data Protection Officer) de leur collectivité . Les contacts sont disponibles dans l'annuaire annexé à la présente charte.

En cas de désaccord sur la manière dont leurs données personnelles sont traitées, les utilisateurs ont également la possibilité de déposer une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) via le site www.cnil.fr.

5. SAVOIR

5.1. ARRIVEE DANS LA COLLECTIVITE OU LE GROUPEMENT DE COLLECTIVITES MEMBRES DU SERVICE COMMUN

Lors de son arrivée, l'utilisateur doit faire le point sur ses besoins avec sa hiérarchie, qui les transmet à la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques pour formaliser ses demandes et dotations en équipements informatiques et de télécommunications.

5.2. ÉQUIPEMENTS INFORMATIQUES ET TELECOMS

L'attribution de moyens de communication ou d'outils informatiques dépend de la fonction et des missions de l'utilisateur. Ces moyens (ordinateur de bureau, PC portable, tablette, téléphone fixe, mobile intelligent, périphériques à mémoire copieurs etc.) évoluent avec le temps et les technologies.

L'utilisateur est personnellement responsable de ces équipements et de leur restitution. Leur usage est professionnel et doit rester conforme aux règles définies par l'administration.

L'utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il doit être raisonnable dans l'utilisation de ces ressources afin d'éviter la saturation ou le détournement à des fins non professionnelles. Les matériels informatiques et téléphoniques qui lui sont confiés sont fragiles et doivent être manipulés avec soin.

5.3. AUTORISATIONS D'ACCES

Les autorisations d'accès fournies à l'utilisateur sont personnelles et incessibles. Elles correspondent à son métier et aux fonctions qu'il exerce et sont limitées à des activités professionnelles. L'utilisateur est responsable de l'utilisation de son compte d'accès au réseau et aux ressources informatiques. Il ne doit en aucun cas communiquer son mot de passe à une tierce personne.

5.4. UTILISATION DES MOYENS DES RESSOURCES INFORMATIQUES ET DE TELECOMMUNICATIONS

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

L'utilisateur est personnellement responsable de l'utilisation des ressources informatiques et de télécommunications de sa collectivité. Il doit contribuer à la sécurité du Système d'Information et ne pas effectuer d'opérations pouvant nuire à son bon fonctionnement ainsi qu'à son intégrité.

5.5. UTILISATION PROFESSIONNELLE

L'utilisation des équipements informatiques et téléphoniques de la collectivité ou de l'établissement public de rattachement est limitée à un usage professionnel. L'utilisation à titre privé est tolérée, mais doit demeurer très occasionnelle et ne doit pas être en contradiction avec les principes déontologiques rappelés dans cette charte.

5.6. PROTECTION DE LA LIBERTE ET DE LA DIGNITE DES PERSONNES

Les contenus illicites, tels que les propos discriminatoires, diffamatoires, pédophiles, ou ceux incitant à la violence ou à la haine raciale, diffusés via Internet, Intranet ou tout autre système de communication de la collectivité, engagent la responsabilité pénale de l'utilisateur.

L'utilisateur dispose du droit au respect de sa vie privée et au secret de ses correspondances. Cependant, l'employeur est en droit de consulter les courriels et SMS présents sur les outils professionnels, sauf s'ils sont expressément identifiés comme personnels. Sans cette mention, les messages sont considérés comme à caractère professionnel.

Pour garantir la sécurité du système d'information, il est crucial de distinguer clairement l'utilisation de la messagerie professionnelle, destinée aux activités liées au travail, de celle personnelle. Les communications personnelles doivent impérativement passer par des dispositifs individuels, tels que les smartphones, et ne doivent pas être consultées sur les postes de travail de la collectivité. Cette précaution vise à éviter les risques de compromission du système d'information, puisque les courriels personnels ne bénéficient pas du même niveau de protection que les courriels professionnels.

Enfin, l'utilisateur ne doit ni lire ni copier les fichiers ou messages d'un autre utilisateur sans autorisation explicite, ni tenter d'intercepter des communications, qu'il s'agisse de messages vocaux, de courriels, de messageries instantanées ou de toute autre forme de communication numérique.

5.7. UTILISATION DES ÉQUIPEMENTS PERSONNELS

L'utilisation d'équipements personnels à des fins professionnelles est généralement interdite pour des raisons de sécurité. Toutefois, dans des cas spécifiques, tels que l'utilisation d'appareils mobiles, des exceptions peuvent être accordées. Dans ce cadre, des mesures pourront être mises en place pour masquer l'affichage des numéros personnels.

Les appareils personnels doivent respecter les standards de sécurité définis par la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques et nécessitent une autorisation préalable. Toutefois, des exceptions peuvent être accordées par la Direction de l'Ingénierie Informatique,

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

des Télécommunications et des Usages Numériques dans des cas spécifiques, tels que l'utilisation de tokens d'authentification pour accéder aux systèmes sécurisés de son employeur.

Les équipements personnels utilisés doivent être conformes aux standards de sécurité définis par la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques, et aucune maintenance ou support technique ne sera assuré par ladite Direction pour ces équipements.

L'utilisateur est entièrement responsable de l'intégrité et de la sécurité des dispositifs personnels utilisés dans le cadre de ses fonctions professionnelles.

5.8. USAGE SOBRE DES OUTILS NUMERIQUES

L'utilisateur doit être conscient de l'impact environnemental du numérique et adopter un comportement vertueux.

Il ne peut prétendre au renouvellement anticipé ou régulier de son matériel numérique. Il appartient à la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques de définir la stratégie de renouvellement des matériels et de juger de leur éventuelle obsolescence.

L'utilisateur doit prendre soin et protéger les matériels qui lui sont confiés afin d'en prolonger la durée de vie. Il doit respecter les procédures communiquées par la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques pour réduire son empreinte environnementale, comme notamment éviter de multiplier les destinataires en copie des mails, ne pas créer de doublons des fichiers, privilégier le partage de liens à l'envoi de fichiers en copie.

L'utilisateur doit veiller à l'extinction quotidienne des moyens numériques lorsqu'il termine son activité et au blocage de ses équipements lorsqu'il ne les utilise pas, notamment pendant les pauses, ou lorsqu'il s'absente de son poste de travail.

5.9. UTILISATION DES SERVICES CLOUD EXTERNES

L'utilisation de services cloud personnels (tels que Dropbox, Google Drive personnel, WeTransfer) est strictement interdite pour le stockage ou le transfert de données professionnelles. Les utilisateurs doivent utiliser les services cloud approuvés par leur employeur ou consulter le service support afin d'envisager la solution de partage la plus adéquates (transferts via serveurs de la mairies ou via des solutions sécurisées déjà déployée en interne comme Teams, SharePoint...

5.10. FORMATION ET SENSIBILISATION

Les utilisateurs doivent participer aux sessions de formation et de sensibilisation organisées par leur employeur. Ces formations ont pour objectif de renforcer leurs compétences en matière de sécurité des systèmes d'information et de protection des données personnelles. La participation régulière à ces formations est essentielle pour maintenir un niveau élevé de sécurité et de conformité.

5.11. SIGNALEMENT DES INCIDENTS

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

Les utilisateurs doivent signaler immédiatement à la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques tout incident de sécurité, suspicion de violation de données, ou toute anomalie constatée.

Un rapport détaillé de l'incident doit être fourni pour permettre une analyse approfondie et la mise en place de mesures correctives. Le signalement se fait en contactant le service support (cf. annuaire en annexe) ou en contactant le RSSI pour des sujets sensibles (cf. annuaire en annexe).

5.12. RESPONSABILITE EN CAS DE PERTE OU DE VOL DE MATERIEL

En cas de perte ou de vol de matériel informatique ou téléphonique, l'utilisateur doit :

- Se rendre au commissariat le plus proche pour faire une déclaration de vol,
- En informer immédiatement la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques en fournissant une copie de la déclaration de vol,
- Collaborer avec ladite Direction ainsi que la Direction des affaires juridiques et le service Assurance pour sécuriser les données et éviter tout usage malveillant du matériel perdu ou volé.

5.13. RESPECT DES POLITIQUES ET PROCEDURES INTERNES

Les utilisateurs doivent se conformer strictement aux politiques et procédures internes de leur collectivité ou établissement public de rattachement.

Ces politiques couvrent divers aspects, tels que l'utilisation des équipements, la gestion des mots de passe, l'accès aux données et la sécurité des informations.

Le non-respect de ces politiques peut entraîner des mesures disciplinaires.

5.14. UTILISATION DES LOGICIELS ET APPLICATIONS

Les logiciels et applications utilisés par les utilisateurs doivent être autorisés et validés par la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques.

L'installation de logiciels non autorisés est interdite.

Les utilisateurs doivent utiliser les logiciels et applications conformément aux licences et aux conditions d'utilisation.

Toute demande d'installation de nouveaux logiciels doit être soumise à la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques pour approbation.

5.15. CONSERVATION ET ARCHIVAGE DES DONNEES

Les utilisateurs doivent veiller à la conservation et à l'archivage appropriés des données professionnelles.

Les données doivent être stockées sur les serveurs sécurisés de leur collectivité et non sur des dispositifs personnels.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

Les procédures de sauvegarde et d'archivage doivent être suivies rigoureusement pour garantir l'intégrité et la disponibilité des données.

5.16. USAGE DE L'INTRANET

L'intranet mis en place par la collectivité est un outil de communication interne et de partage de ressources, destiné à faciliter le travail collaboratif, l'accès à l'information, et la diffusion des actualités et directives importantes.

L'intranet mis en place par la collectivité est un outil de communication interne et de partage de ressources, conçu pour faciliter le travail collaboratif, l'accès à l'information, et la diffusion des actualités et directives importantes. Son utilisation est strictement réservée aux activités professionnelles et doit servir les missions de la collectivité.

L'usage de l'intranet doit être conforme aux règles établies, notamment en ce qui concerne la diffusion des contenus. Toute information publiée doit être pertinente, exacte, et validée conformément aux directives internes. Les utilisateurs ont la responsabilité de s'assurer de la véracité des informations avant de les partager et doivent éviter de poster des contenus inappropriés, sensibles ou non sécurisés. En cas de partage de documents, il est essentiel de garantir qu'ils ne comportent pas de failles de sécurité ou de logiciels malveillants.

Les interactions sur l'intranet doivent être empreintes de respect, de neutralité, et de non-discrimination. Les commentaires ou communications injurieuses, offensantes ou diffamatoires sont interdits, et les utilisateurs sont encouragés à interagir de manière professionnelle et courtoise. Le non-respect de ces règles peut entraîner des sanctions appropriées.

Concernant l'accès, certaines sections de l'intranet peuvent être restreintes selon les fonctions et les responsabilités de chaque utilisateur. Il est essentiel de respecter ces limitations et de ne pas tenter d'accéder à des zones non autorisées. Les identifiants de connexion, qui permettent l'accès sécurisé, sont personnels et confidentiels. Leur partage avec d'autres personnes est strictement interdit.

Il est recommandé de consulter régulièrement l'intranet pour se tenir informé des mises à jour et des nouveautés. Les utilisateurs doivent aussi suivre les bonnes pratiques en matière de gestion des fichiers, en veillant à organiser les documents de manière claire et à supprimer ceux qui sont obsolètes pour éviter l'encombrement. Lors des périodes de maintenance, des interruptions de service peuvent survenir, et des notifications seront émises pour en informer les utilisateurs.

Enfin, l'usage de l'intranet constitue une responsabilité partagée, et chacun doit contribuer à assurer la sécurité et l'efficacité de cet outil tout en protégeant les informations sensibles de la collectivité.

6. UTILISATION RESPONSABLE D'INTERNET ET DES OUTILS NUMERIQUES

6.1. COMPORTEMENT RESPONSABLE EN LIGNE

Il est impératif pour l'utilisateur territorial de se comporter comme un internaute responsable.

Internet, comme tous les moyens mis à disposition par l'administration, est destiné à un usage strictement professionnel. L'usage privé doit rester accessoire. Sur Internet, tout comme dans l'exercice de ses

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

fonctions, l'utilisateur doit faire preuve de professionnalisme, de discernement, de bon sens, de courtoisie, et de prudence, tout en respectant les lois et réglementations en vigueur.

L'utilisation d'Internet doit toujours être conforme à la législation, aux règlements, aux bonnes mœurs, et à la politique de la collectivité. L'agent est tenu de respecter les droits et obligations des fonctionnaires, en adoptant un comportement en ligne qui reflète ces valeurs. Cela inclut la dignité, en veillant à ne pas nuire à l'image de l'administration ; l'impartialité, en restant exempt de tout préjugé ; l'intégrité, en accomplissant ses fonctions de manière désintéressée ; et la probité, en s'abstenant de tirer un profit personnel de ses missions.

6.2. TELECHARGEMENTS : PRUDENCE ET SECURITE

Les téléchargements peuvent perturber sérieusement le fonctionnement du Système d'Information des collectivités ou des groupements de collectivités membres du service commun. Cela peut entraîner des ralentissements d'accès pour les autres utilisateurs, impacter l'utilisation des applications métiers, causer des problèmes de gestion des espaces disques, créer des incompatibilités logicielles, ou introduire des virus. De plus, les données circulant sur Internet peuvent être réglementées en termes d'utilisation ou protégées par un droit de propriété intellectuelle. Les téléchargements représentent donc un vecteur de transmission important de virus.

Il est impératif de ne télécharger que des ressources fiables depuis des sites de confiance. De même, l'installation de logiciels « crackés », piratés ou sans licence est strictement interdite. En cas de doute sur la sécurité ou la légitimité d'un téléchargement ou en cas d'incident potentiel, il est obligatoire de demander l'avis du Service support.

6.3. FILTRAGE INTERNET

L'accès Internet est un outil professionnel. Les collectivités et le groupement de collectivités membres du service commun mettent en place des mesures d'analyse et de filtrage des flux réseaux pour garantir la sécurité du système d'information :

- Éviter le téléchargement de données malveillantes,
- Filtrer l'accès à des sites dont la catégorisation est inappropriée,
- Contrôler les fuites de données vers l'extérieur,
- Ne pas utiliser les réseaux métropolitains pour des besoins strictement privés ou récréatifs.

Ces outils de filtrage concernent tous les utilisateurs avec des droits d'accès attribués par groupe, basés sur l'identification des sites accédés et sur une analyse automatisée des flux circulants.

Le filtrage des d'accès aux sites se base sur :

- La catégorisation du site,
- Une liste blanche de sites autorisés,
- Une liste noire de sites exclus.

Un utilisateur peut demander l'ouverture d'un site en liste blanche en contactant l'administration, qui évaluera la demande en fonction des missions de l'utilisateur et des contraintes de sécurité.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

L'analyse automatisée des flux exclut l'inspection des données avec des sites relevant du secteur bancaire ou du domaine de la santé. Ce contrôle s'opère sur tout équipement professionnel, qu'il soit utilisé depuis le réseau interne de la collectivité ou depuis un réseau privé (domicile en télétravail par exemple).

La loi interdit l'accès à des sites de nature diffamatoire, discriminatoire, raciste, sexiste, révisionniste, pédophile ou incitant à la violence ou à la haine raciale. En cas d'agissements de cette nature, la responsabilité pénale personnelle de l'utilisateur peut être engagée, indépendamment des sanctions disciplinaires.

6.4. INTERDICTION DE CONTOURNER LES OUTILS DE SECURITE

Pour garantir la sécurité du Système d'Information du service commun « Informatique, Télécommunications et Usages Numériques » , il est formellement interdit aux utilisateurs de :

- Contourner ou désactiver les outils de sécurité mis en place, tels que le pare-feu, les antivirus, les systèmes de détection d'intrusion ou autres dispositifs de protection
- Utiliser des outils pour masquer leur navigation sur Internet, tels que les VPN non autorisés, les proxys anonymes ou tout autre logiciel permettant de dissimuler l'activité en ligne
- Installer des logiciels ou des applications non autorisés par la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques. Toute demande d'installation de nouveaux logiciels doit être approuvé par celle-ci,
- Octroyer ou tenter d'octroyer des droits d'accès ou des permissions auxquels ils n'ont pas été expressément autorisés. Cela inclut l'utilisation de comptes administratifs ou l'élévation de privilèges sans approbation officielle
- Télécharger de manière illicite et illégale des fichiers, y compris des logiciels, des vidéos, de la musique ou tout autre contenu protégé par des droits d'auteur.
- Télécharger des fichiers ou des logiciels à partir de sources non sécurisées ou non autorisées, ce qui pourrait introduire des virus ou des logiciels malveillants dans le système.
- Désactiver ou tenter de désactiver l'authentification à double facteur (2FA) ou tout autre mécanisme de sécurité supplémentaire mis en place pour protéger les comptes et les données sensibles.

Les utilisateurs doivent utiliser les outils et logiciels fournis conformément aux directives et aux politiques de sécurité du service commun « Informatique, Télécommunications et Usages Numériques » Toute tentative de contourner ces mesures de sécurité pourra être considérée comme une faute grave.

6.5. USAGE DE L'INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle (IA) simule certains traitements de l'intelligence humaine en créant et appliquant des algorithmes dans un environnement informatique dynamique.

Les collectivités et le groupement de collectivités membres du service commun s'engagent à respecter des principes éthiques dans l'usage de ces algorithmes : Transparence, Équité, Maîtrise Humaine, Durabilité et Sûreté. Les outils numériques reposant sur l'IA et développés par les collectivités et le groupement de collectivités membres du service commun respectent ces engagements.

Les utilisateurs doivent utiliser les outils mis à disposition en respectant ces principes éthiques. Il est interdit d'utiliser des outils tiers basés sur l'IA qui exfiltrent des données des collectivités ou groupement de collectivités membres du service commun. Ces outils peuvent s'approprier les données et leurs conditions de réutilisation ne sont pas garanties. L'utilisateur ne doit pas demander à ces moteurs d'IA

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 17/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

d'analyser des données professionnelles ou de préparer des analyses contextuelles avec des éléments du domaine professionnel car cela pourrait entraîner la fuite de données sensibles.

6.6. PRATIQUES DE SECURITE POUR LE NOMADISME NUMERIQUE

Dans le cadre de leurs missions, les utilisateurs territoriaux peuvent être amenés à travailler à distance ou en déplacement, ce qui inclut l'utilisation de dispositifs mobiles (ordinateurs portables, tablettes, smartphones). Afin d'assurer la sécurité des données dans ces situations, il est essentiel de respecter les bonnes pratiques du nomadisme numérique :

- Utilisation de réseaux sécurisés : Les connexions à Internet depuis des réseaux publics non sécurisés (par exemple, des réseaux Wi-Fi publics) doivent être évitées. Lorsqu'une connexion publique est nécessaire, l'utilisation d'un VPN approuvé par la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques est obligatoire pour protéger les données échangées.
- Chiffrement des données : Les documents sensibles doivent être stockés et transférés en utilisant des supports de stockage chiffrés (clés USB sécurisées, disques durs chiffrés). Les connexions doivent aussi être sécurisées par un protocole de chiffrement (HTTPS, TLS).
- Authentification renforcée : L'utilisation de l'authentification à double facteur (2FA) est obligatoire pour accéder aux systèmes d'information à distance. Cela garantit un niveau de protection supplémentaire en cas de vol ou de perte du dispositif.
- Sauvegardes régulières : Les utilisateurs doivent s'assurer que leurs fichiers sont sauvegardés régulièrement sur des supports sécurisés ou sur le cloud mis à disposition par leur collectivité.
- Mise à jour des systèmes et logiciels : Les dispositifs utilisés en déplacement ou en télétravail doivent être régulièrement mis à jour pour garantir leur sécurité. Les utilisateurs doivent s'assurer que les logiciels installés disposent des derniers correctifs de sécurité, en acceptant le téléchargement des derniers patchs de sécurité.
- Verrouillage des sessions : En déplacement ou en télétravail, les sessions de travail doivent être verrouillées lorsque l'utilisateur s'éloigne de son dispositif pour empêcher tout accès non autorisé.

L'ensemble de ces mesures a pour objectif de garantir la continuité et la sécurité des services tout en protégeant les informations sensibles, conformément aux engagements de leur employeur en matière de cybersécurité et de protection des données.

6.7. SECURITE PHYSIQUE ET ACCES AUX LOCAUX

La sécurité physique des équipements est primordiale. Les utilisateurs doivent :

- S'assurer que les visiteurs sont correctement identifiés et enregistrés.
- Respecter les procédures d'accès aux zones sensibles et verrouiller leurs postes de travail lorsqu'ils sont laissés sans surveillance.

7. UTILISATION DES OUTILS COLLABORATIFS

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

7.1. LA MESSAGERIE

7.1.1. UTILISATION DE LA MESSAGERIE À DES FINS PROFESSIONNELLES

La messagerie est destinée à un usage strictement professionnel.

La diffusion de messages à caractère privé doit rester occasionnelle et limitée. Les utilisateurs doivent respecter les circuits organisationnels et la voie hiérarchique le cas échéant. Si un message est reçu par erreur, il doit être signalé à l'expéditeur. Les utilisateurs de la messagerie sont informés de l'existence de modérateurs (filtres), dans le but d'assurer la sécurité des réseaux informatiques et de limiter les risques d'abus d'une utilisation trop personnelle.

Il est interdit de tenter de lire ou copier les courriels d'un autre utilisateur sans son autorisation expresse. Toute tentative d'interception de courriels entre utilisateurs sans autorisation est également proscrite.

L'utilisation de la messagerie à des fins privées est tolérée uniquement lorsqu'elle est nécessaire pour des raisons personnelles ou familiales urgentes, à condition que cela n'affecte pas le bon fonctionnement de la messagerie professionnelle.

Par défaut, tout courriel envoyé ou reçu à partir du poste de travail mis à disposition par l'employeur est considéré comme professionnel.

Il est interdit de transférer des courriels professionnels sur une boîte mail privée sans autorisation du responsable.

En cas d'absence prolongée et pour les besoins du service, la collectivité peut accéder à la messagerie professionnelle de l'utilisateur. Cet accès peut être autorisé par le responsable hiérarchique, après avis du délégué à la protection des données (DPO).

Seuls les courriels privés identifiés comme tels sont protégés au titre du respect de la vie privée et du secret des correspondances. La collectivité ne peut pas accéder aux courriels privés, sauf dans le cadre d'une procédure d'enquête judiciaire ou sur autorisation d'un juge. Pour que les courriels privés soient protégés, ils doivent être identifiés comme tels, par exemple :

- En précisant dans leur objet « Personnel » ou « Privé »,
- En les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

Afin de protéger la sécurité et l'intégrité des systèmes informatiques, il est essentiel que tous les utilisateurs respectent les directives suivantes concernant l'utilisation de leurs adresses email professionnelles :

- Les utilisateurs doivent éviter de communiquer leur adresse email professionnelle sur des sites ou des plateformes non approuvés par l'entreprise.
- L'adresse email professionnelle ne doit être utilisée que pour des communications liées au travail et des contacts professionnels.
- Les utilisateurs ne doivent pas s'inscrire à des newsletters ou des services en ligne avec leur adresse email professionnelle sans une autorisation préalable de leur supérieur hiérarchique ou de la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques.
- Toute inscription à une newsletter ou à un service en ligne doit être en lien direct avec les besoins professionnels de l'utilisateur.
- Les utilisateurs doivent être vigilants quant aux emails reçus et éviter d'ouvrir des pièces jointes ou de cliquer sur des liens provenant d'expéditeurs inconnus.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

- En cas de réception d'un email suspect, les utilisateurs doivent immédiatement le signaler à la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques.
- Il est interdit de transmettre des informations confidentielles ou sensibles par email à des entités externes sans une autorisation appropriée.
- Les utilisateurs doivent s'assurer que leur boîte mail professionnelle est protégée par un mot de passe sécurisé et régulièrement mis à jour.

En suivant ces directives, nous pouvons garantir une utilisation sécurisée et appropriée des adresses email professionnelles, réduisant ainsi les risques liés à la sécurité et aux pertes de données.

7.1.2. GESTION DES MESSAGES VOLUMINEUX

Afin de renforcer la sécurité et l'efficacité du partage de fichiers, l'utilisation de fichiers ZIP pour l'envoi de fichiers volumineux par messagerie est interdite. Les utilisateurs sont tenus d'utiliser les solutions collaboratives mises à disposition par l'employeur, à savoir Teams, OneDrive, ou SharePoint, les lecteurs réseau ou partage de fichiers ou enregistrés sur les serveurs pour le partage et le transfert de ces fichiers.

Cette approche assure une meilleure gestion des données, réduit les risques liés à la compression des fichiers, et facilite le suivi et la sécurisation des échanges. Les utilisateurs doivent se familiariser avec les procédures de partage via ces plateformes pour garantir leur conformité avec cette directive.

Lorsque le destinataire accède au même serveur de fichiers (en principe même direction), il peut être plus judicieux d'envoyer un lien ou un raccourci plutôt que le fichier lui-même.

7.1.3. PRUDENCE ET PROFESSIONNALISME DANS L'ENVOI DE COURRIELS

Les utilisateurs peuvent être victimes d'émetteurs indélicats ou recevoir par exemple des courriers non sollicités de nature commerciale, malveillante, raciste, propagandiste, etc. (spamming). En cas de doute, ils doivent s'adresser au service support de la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques.

De manière générale, il est conseillé d'éviter de s'inscrire à des listes de diffusion incertaines.

Il faut être vigilant contre l'hameçonnage : ne pas ouvrir les courriels au contenu suspect, ni cliquer sur des liens douteux. Pour éviter les intrusions et la propagation de virus, il ne faut jamais ouvrir des pièces jointes suspectes (émetteur inconnu, fichiers .exe). Il est préférable de supprimer ces messages puis de vider le dossier « éléments supprimés ».

La Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques peut bloquer ponctuellement certains types de fichiers joints ou supprimer des messages dangereux identifiés dans toutes les boîtes mails de la collectivité. Tout courriel malveillant doit être signalé à la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques.

Pour les modalités de contact il y a lieu de se référer à l'annuaire repris en annexe.

7.1.4. PARTAGE DE DOCUMENTS

Pour partager des documents avec des destinataires internes ou externes, les utilisateurs doivent contacter le service support pour connaître les solutions validées par leur employeur.

Les précautions suivantes doivent être appliquées pour éviter que des données confidentielles ne soient exposées à l'extérieur de l'organisation :

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

- Bien organiser les données pour avoir une vision claire des documents et des partages associés,
- Être vigilant sur les éléments partagés selon leur degré de confidentialité,
- Assurer le suivi de la gestion des droits d'accès accordés, et exiger l'authentification des destinataires,
- Être vigilant sur les fichiers tiers partagés.

7.1.5. LES MODÉRATEURS

Dans certaines collectivités, des modérateurs ont été mis en place pour assurer le contrôle de la diffusion de certains contenus et pour garantir que l'information partagée respecte les règles établies. Les règles de modérations sont définies pour chaque collectivité.

7.2. UTILISATION DES RESEAUX SOCIAUX

7.2.1. Objectifs de l'utilisation des réseaux sociaux

Les réseaux sociaux sont des outils de communication essentiels pour diffuser des informations officielles, promouvoir les actions de la collectivité et faciliter l'interaction avec les citoyens et les parties prenantes. Leur utilisation doit être encadrée pour garantir la cohérence des communications, la sécurité des informations et le respect des valeurs de la collectivité.

Les collectivités et établissements publics de coopération intercommunale communiquent régulièrement via les médias traditionnels (presse écrite, radio, TV) et les réseaux sociaux. Ils peuvent disposer pour ce faire :

- d'un compte Facebook : destiné au grand public et plus particulièrement aux habitants du territoire, sont diffusées sur ce compte toutes les informations relatives à l'activité des collectivités et établissements publics de coopération intercommunale : informations pratiques, vie de la collectivité, actualités, messages de prévention... ;
- d'un compte Twitter : pour une diffusion régulière d'informations instantanées, principalement à destination des journalistes et institutionnels ;
- d'un compte Linkedin : davantage destiné aux institutionnels, décideurs et chefs d'entreprises. Ils valorisent l'image de marque de la collectivité ;
- d'un compte Instagram : qui fait la part belle aux photos et à l'image. Cible : grand public ;
- d'une chaîne Youtube : dédiée aux vidéos ;

Ces différents comptes sont gérés et administrés au sein d'une direction de la communication.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

7.2.2. Communication des missions professionnelles

Les utilisateurs ne doivent pas communiquer sur leurs missions professionnelles ou partager des informations relatives à leurs projets sans l'aval préalable de leur responsable hiérarchique ou du service communication.

Toute communication liée aux missions professionnelles doit être soumise au service communication pour validation avant diffusion. Cela inclut, mais sans s'y limiter, les publications concernant les projets en cours, les initiatives locales, et les collaborations externes.

Les utilisateurs sont autorisés à relayer des informations officielles publiées par leur collectivité, sous réserve de n'y apporter aucune modification et de veiller à toujours intégrer l'origine de la communication. Il est essentiel de s'assurer que ces informations proviennent de sources officielles et sont conformes aux directives du service communication.

7.2.3. Devoir de neutralité et de discernement

Tous les utilisateurs —titulaires de la fonction publique ou contractuels— sont soumis au devoir de réserve et doivent donc faire preuve de retenue et de mesure dans leurs publications, quelles qu'elles soient, lorsque celles-ci concernent leur activité professionnelle ou l'institution. Chaque utilisateur est responsable du contenu de ses publications.

Les utilisateurs doivent maintenir une neutralité stricte dans leurs communications sur les réseaux sociaux, évitant toute prise de position personnelle qui pourrait être perçue comme représentant la collectivité. Il est essentiel de faire preuve d'une discrétion exemplaire dans toutes les interactions en ligne, en veillant à ne pas divulguer d'informations sensibles ou destinées à un usage interne. Les communications doivent toujours incarner les valeurs de la collectivité, telles que le respect, l'intégrité et le professionnalisme. Le devoir de réserve s'applique à tous les utilisateurs, y compris dans leur sphère privée.

Ce que peuvent faire les utilisateurs sur leurs comptes personnels :

- Liker et commenter les publications de leur collectivité ou établissement public de coopération intercommunale sur leurs réseaux.
- Partager les publications de leur collectivité ou établissement public de coopération intercommunale sur leurs réseaux.
- Mentionner dans leur profil leurs fonctions au sein de leur collectivité ou établissement public de coopération intercommunale.
- Identifier des personnes sur les posts de leur collectivité ou établissement public de coopération intercommunale.
- Partager des publications faisant mention du travail mené avec leur collectivité ou établissement public de coopération intercommunale.
- Évoquer leur mission au sein de la collectivité dans le respect des valeurs portées par leur collectivité ou établissement public de coopération intercommunale.

Ce que ne peuvent pas faire les utilisateurs :

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

- Utiliser le logo et la charte graphique de leur collectivité ou établissement public de coopération intercommunale sur leurs comptes comme éléments d'identification (photo de couverture, de profil...). Le logo et la charte graphique de la collectivité ne peuvent être utilisés que par l'institution.

- S'exprimer au nom de leur collectivité ou établissement public de coopération intercommunale : seuls les élus qui portent les politiques communautaires et la direction de la Communication (sauf accord formel de celle-ci) sont habilités à parler au nom de la collectivité.

- Reprendre à leur compte des posts de leur collectivité ou établissement public de coopération intercommunale (ne pas partager mais copier-coller comme s'ils en étaient l'émetteur).

- Commenter ou répondre aux critiques éventuelles à l'encontre de leur collectivité ou établissement public de coopération intercommunale dans les commentaires.

- Publier du contenu qui porterait préjudice à la collectivité : dénigrer une politique, un(e) élu(e), une réalisation, une action, un service ou un utilisateur...

Les utilisateurs sont régulièrement sollicités par la direction de la Communication lorsqu'il est nécessaire d'apporter une réponse à certains commentaires ou questions. Le fonctionnement des réseaux sociaux exigeant de la réactivité, il est indispensable que la direction de la Communication puisse obtenir rapidement les éléments afin de formuler une réponse à l'usager dans les plus brefs délais.

7.2.4. Gestion des comptes officiels

Les comptes officiels de la collectivité sur les différentes plateformes de réseaux sociaux (Facebook, Twitter, LinkedIn, Instagram, etc.) sont gérés exclusivement par des utilisateurs désignés par le service communication.

L'accès aux comptes officiels doit être sécurisé et limité aux utilisateurs autorisés. Les identifiants et mots de passe doivent être protégés et ne doivent pas être partagés avec des personnes non autorisées. En cas de compromission des accès, il faut immédiatement en informer la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques.

7.2.5. Modération et gestion des contenus

Les utilisateurs responsables des comptes officiels doivent surveiller et modérer les commentaires et interactions pour garantir un environnement respectueux et constructif. Les contenus inappropriés, diffamatoires, discriminatoires ou incitant à la haine doivent être supprimés conformément aux politiques de modération établies.

En cas de crise ou de situation délicate, les utilisateurs doivent suivre les procédures établies par la collectivité pour la gestion des communications sur les réseaux sociaux, afin de maintenir une communication cohérente et respectueuse.

7.3. PROPRIETE DES DONNEES

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

Les données produites dans un cadre professionnel sont la propriété de la collectivité, quel que soit leur format :

- Message électronique,
- Fichier bureautique,
- Photographie (sous réserve de consentement préalable)
- Film,
- Dessin,
- Coordonnée géographique, etc.

Ces données peuvent être partagées, dans le respect de la règlementation en vigueur, uniquement avec les autres utilisateurs habilités et susceptibles de travailler sur les mêmes dossiers. Les documents et les données produits doivent être enregistrés sur les serveurs de la collectivité ou sur les applicatifs métiers (One Drive, Share point, Teams), en veillant à :

- Enregistrer ces données dans un répertoire adapté, limitant leur accès aux personnes habilitées,
- Ne pas copier ces données plusieurs fois pour éviter d'accroître l'espace de stockage.

8. UTILISATION DE LA BUREAUTIQUE

8.1. LA SECURITE : UNE RESPONSABILITE PARTAGEE

D'une manière générale, la sécurité informatique consiste à s'assurer que les ressources matérielles et logicielles de l'entreprise sont uniquement utilisées dans le cadre prévu à cet effet afin de limiter les risques. La sécurité informatique vise donc à garantir l'intégrité, la confidentialité des données ainsi que la disponibilité du Système d'Information.

L'homogénéité des postes de travail est une condition indispensable pour maîtriser l'intégration des composants, leur déploiement et leur administration :

- Chaque poste de travail correspond à une configuration type, adaptée au profil professionnel de l'utilisateur (applications auxquelles il a accès). Si une réinstallation est nécessaire, elle sera faite sur la base de cette configuration répertoriée.
- Les utilisateurs sont responsables de l'utilisation des ressources informatiques ; ils ne doivent pas effectuer d'opérations pouvant nuire au bon fonctionnement des systèmes et à leur intégrité (par exemple, intervention sur des fichiers systèmes).

8.2. IDENTIFIANTS DE CONNEXION : CODE D'ACCES AU SYSTEME D'INFORMATION

- Les identifiants de connexion sont composés du nom d'utilisateur (login) et d'un mot de passe, et permettent de gérer la confidentialité des données.
- Ces identifiants sont personnels et ne doivent en aucun cas être communiqués à d'autres utilisateurs qui pourraient les utiliser pour nuire à l'intégrité des données dont l'utilisateur a la responsabilité.
- Pour renforcer cette confidentialité, les mots de passe doivent être changés régulièrement conformément aux modalités définies par le responsable de la sécurité de l'information, accessibles sur intranet.

8.3. ENGAGEMENTS DE L'UTILISATEUR :

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

L'utilisateur s'engage à :

- Ne pas masquer sa véritable identité ;
- Ne pas usurper l'identité d'autrui ;
- Ne pas quitter son poste de travail en laissant celui-ci accessible ;
- Signaler au service support utilisateur toute violation ou tentative de violation suspectée de son compte informatique, ainsi que toute anomalie constatée (problèmes d'initialisation, mauvais fonctionnement, etc.) ;
- Ne pas introduire de « ressources extérieures » matérielles ou logicielles pouvant porter atteinte à la sécurité du Système d'Information ;
- Éteindre son poste de travail en fin d'activité.

En cas de besoin d'accéder à une nouvelle application, il convient de faire la demande auprès du service support.

8.4. PREVENTION DES VIRUS

Les virus représentent une menace majeure pour la sécurité et l'intégrité du réseau de la collectivité. Les serveurs et les postes de travail sont équipés d'antivirus pour prévenir ces risques. Il est crucial de vérifier la fiabilité des fichiers provenant de sources extérieures et se connectant au réseau. Une attention particulière doit être portée aux clés USB dont la provenance est inconnue.

La Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques met en place un ensemble d'outils de sécurisation, et il est strictement interdit de désactiver les systèmes de protection des postes de travail. En cas de doute concernant l'origine, la taille, le type de fichier ou l'objet d'un message, l'utilisateur doit :

- Relever un maximum d'éléments caractéristiques pour permettre une analyse précise de l'incident (par exemple, capture d'écran du message d'erreur, courriel infesté, etc.) ;
- Ne pas utiliser le fichier ou le message suspect et contacter le Service support.

8.5. UTILISATION DES FICHIERS

Les utilisateurs ne doivent pas tenter de lire ou copier les fichiers d'un autre utilisateur sans son autorisation expresse. Par défaut, les fichiers présents sur les serveurs, dans le cloud ou sur les postes de travail sont considérés comme professionnels et peuvent être consultés librement par l'administration, y compris en dehors de la présence de l'utilisateur.

Seuls les fichiers privés identifiés comme tels sont protégés au titre du respect de la vie privée ; la collectivité ne peut accéder à ces fichiers privés qu'en présence de l'utilisateur, après l'avoir informé, ou en cas de risque ou d'événement particulier. Pour protéger ces fichiers privés, ils doivent être identifiés comme tels, par exemple :

- En précisant dans leur nom « Personnel » ou « Privé »,
- En les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

Les utilisateurs doivent éviter de stocker des fichiers sur leurs postes de travail et privilégier autant que possible le stockage et l'enregistrement sur le serveur de la collectivité.

8.6. NETTOYAGE DES SERVEURS DE FICHIERS

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

Afin de garantir une gestion efficace des données et d'optimiser l'utilisation des ressources de stockage, il est obligatoire de procéder à un nettoyage annuel des serveurs de fichiers.

Chaque année, les responsables des services doivent s'assurer que les fichiers obsolètes, inutilisés, ou non conformes aux politiques de conservation des données soient identifiés et supprimés. Ce processus doit être réalisé en collaboration avec la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques pour s'assurer que les bonnes pratiques en matière de sécurité et d'archivage soient respectées.

Cette démarche vise à prévenir l'encombrement des serveurs, à réduire les coûts de stockage, et à garantir la disponibilité des données pertinentes.

En complément des directives existantes, la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques se réserve le droit de supprimer tout fichier non conforme aux usages professionnels stockés sur les serveurs de la collectivité. De plus, les fichiers qui n'ont pas été utilisés depuis une période de deux ans seront identifiés pour suppression afin de garantir une gestion optimale de l'espace de stockage. Cette suppression sera soumise à l'autorisation de l'utilisateur. Les utilisateurs sont responsables de la gestion de leurs fichiers et doivent veiller à transférer tout fichier personnel vers un espace de stockage privé avant la mise en œuvre de cette politique.

8.7. SOBRIETE NUMERIQUE ET IMPACT ENVIRONNEMENTAL

Les utilisateurs doivent adopter un comportement responsable pour limiter l'impact environnemental de leur usage des outils numériques. La sobriété numérique vise à réduire la consommation d'énergie, l'utilisation excessive des ressources informatiques, et la production de déchets électroniques tout en maintenant l'efficacité des services.

Pour promouvoir cette démarche, les utilisateurs sont invités à :

- **Réduire les envois et stockages inutiles :** privilégier le partage de liens vers des documents plutôt que l'envoi de pièces jointes, limiter les destinataires en copie des emails, et supprimer régulièrement les fichiers ou emails obsolètes.
- **Limiter les impressions :** n'imprimer que lorsque nécessaire et utiliser les fonctionnalités d'impression recto-verso et noir et blanc par défaut.
- **Optimiser l'utilisation des équipements :** éteindre les équipements (ordinateurs, écrans, imprimantes) en fin de journée et les débrancher lorsqu'ils ne sont pas utilisés pendant une longue période.
- **Utiliser des outils collaboratifs partagés :** stocker les documents sur les serveurs ou les espaces de collaboration validés (Teams, OneDrive, SharePoint) plutôt que sur des supports locaux ou personnels.
- **Favoriser la durabilité des équipements :** manipuler avec soin les appareils mis à disposition et signaler tout dysfonctionnement pour éviter leur détérioration.
- **Se former :** suivre les formations proposées pour mieux comprendre l'impact environnemental du numérique et adopter des pratiques écoresponsables.

En adoptant ces pratiques, chaque utilisateur contribue à réduire l'empreinte écologique de la collectivité tout en optimisant les ressources numériques. La Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques pourra effectuer des campagnes de sensibilisation pour accompagner cette transition vers une sobriété numérique.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

8.8. PRISE EN MAIN A DISTANCE

Aux fins de maintenance informatique, les techniciens habilités de la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques peuvent accéder à distance à l'ensemble des données de n'importe quel poste de travail informatisé ainsi qu'à la session de travail en cours.

Cette prise de contrôle à distance s'effectue avec l'autorisation expresse de l'utilisateur, sauf en l'absence de ce dernier et en cas de nécessité technique d'accès à cet ordinateur. Dans cette dernière hypothèse, la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques procède obligatoirement à la réinitialisation du mot de passe de session. L'utilisateur est alors informé de l'intervention lors de la transmission du nouveau mot de passe par la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques.

9. TELEPHONIE

9.1. MAITRISE DU TEMPS DE COMMUNICATION

L'usage des téléphones est réservé aux besoins professionnels.

Un usage ponctuel du téléphone pour des communications personnelles est toléré à condition que cela n'entrave pas l'activité professionnelle. Les utilisateurs doivent respecter les usages et maîtriser les dépenses liées aux communications téléphoniques.

9.2. UTILISATION D'UN TELEPHONE MOBILE PROFESSIONNEL

Les utilisateurs dotés d'un téléphone mobile professionnel doivent connaître les limites de leur forfait. En cas de doute, ils doivent consulter le support utilisateur pour obtenir les caractéristiques de leur forfait (durée, options, etc.) et veiller à respecter le cadre prévu par celui-ci.

Les appels vers les numéros de services commençant par 08 (hors numéros gratuits), les appels depuis ou vers l'étranger, et les téléchargements de sonneries et autres logos sont facturés hors forfait et seront à la charge de l'utilisateur.

L'utilisateur doit signaler au support utilisateur tous les cas de dysfonctionnements, de casse, de perte, de vol, de difficultés d'utilisation ou de changement de situation. L'utilisation du téléphone portable est liée à l'emploi de l'utilisateur, par conséquent, tout changement de fonction peut entraîner la reprise de l'équipement.

9.3. CONSOMMATION TELEPHONIQUE

Pour chaque ligne téléphonique, une facture détaillée anonymisée des numéros composés par l'utilisateur peut être éditée et transmise à son responsable hiérarchique. Poste par poste, les dates et heures des appels sortants, ainsi que les durées, les coûts et numéros appelés, sont stockés et conservés pendant la durée maximale légale afin de permettre le contrôle des factures, le suivi statistique et la réalisation d'études en vue de la réduction des coûts ou d'un meilleur dimensionnement du service. Ce suivi est effectué tant pour le téléphone fixe que pour les mobiles.

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

10. DEPART D'UN UTILISATEUR OU GESTION DES DROITS D'ACCES EN CAS D'ABSENCE PROLONGEE

Lorsqu'un utilisateur quitte définitivement la collectivité ou est absent de manière prolongée (congé parental, congé maternité, congé longue durée, congé longue maladie, etc.), il doit prendre les mesures suivantes pour assurer la continuité du service et la restitution des équipements. Les démarches incluent la gestion des droits d'accès, des matériels informatiques et des données professionnelles.

10.1. PREPARATION DU DEPART OU DE L'ABSENCE PROLONGEE

L'utilisateur doit anticiper son départ en informant ses interlocuteurs ainsi que son responsable. Le service des Ressources Humaines notifie le service support de ce départ ou de l'absence imminente. Il est conseillé de favoriser l'utilisation des ressources partagées (serveurs de fichiers bureautiques, boîte mail partagée, intranet) afin d'assurer la continuité des activités et de minimiser les interruptions de service.

10.2. RESTITUTION DES EQUIPEMENTS ET MATERIELS

Avant de partir ou lors d'une absence prolongée, l'utilisateur doit organiser la restitution de tous les équipements mis à sa disposition (ordinateur, téléphone mobile, tablette, accessoires, etc.) auprès de la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques. Celle-ci se chargera de reconfigurer et d'effacer les données personnelles des équipements pour les préparer à une réutilisation.

10.3. MESSAGERIE ET GESTION DES FICHIERS

À la fin de l'emploi de l'utilisateur, le compte est désactivé immédiatement et est supprimé dans un délai maximum de trois mois, sauf en cas d'exception. Avant cette échéance, l'utilisateur doit s'assurer de supprimer ses messages privés ou personnels. Après le départ, la collectivité pourra accéder aux messages professionnels restants pour assurer la continuité du service.

L'utilisateur doit sauvegarder tous ses fichiers professionnels sur l'espace partagé de sa direction avant son départ. Les documents et données créés dans le cadre professionnel restent la propriété de la collectivité. Il est interdit de copier ou d'emporter ces documents hors de l'institution. Le poste de travail de l'utilisateur pourra être réutilisé après son départ sans son consentement.

10.4. TELEPHONIE ET SUSPENSION DES LIGNES

L'utilisateur doit contacter le support utilisateur pour suspendre sa ligne mobile professionnelle et rendre les équipements téléphoniques. Il doit également supprimer toutes les informations personnelles des équipements mobiles, car ces derniers seront réutilisés.

10.5. GESTION DES DROITS D'ACCES EN CAS DE DEPART DEFINITIF OU D'ABSENCE PROLONGEE

Lorsque l'utilisateur quitte définitivement la collectivité (fin de contrat, départ en retraite, démission, mutation, décès), ses comptes sont désactivés dès son départ et supprimés au bout de 30 jours, à moins qu'un litige juridique ne soit en cours. Toutes les habilitations, y compris les droits d'accès aux logiciels

Envoyé en préfecture le 17/12/2025
Reçu en préfecture le 17/12/2025
Publié le 19/12/2025
ID : 062-216207530-20251215-D_2025_1215_10-DE

payants et la boîte mail, sont également révoquées. Il est recommandé que l'utilisateur programme un message d'absence pour indiquer son départ et faciliter le suivi des dossiers restants.

En cas d'absence prolongée, le manager de l'utilisateur peut demander l'accès aux documents stockés sur ses équipements, en accord avec la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques et après validation par le Directeur ou le RSSI. Si cela est possible, le consentement de l'utilisateur absent sera recueilli, sinon, la demande sera tracée par le DPD. Le manager informera ensuite l'utilisateur des documents consultés.

Enfin, la suppression des habilitations aux logiciels payants et autres droits peut être demandée pendant une absence prolongée, et les équipements peuvent être réassignés à un remplaçant sous validation managériale.

11. ENQUETE ADMINISTRATIVE INTERNE

En cas d'ouverture d'une enquête administrative interne décidée par le Directeur général des services de la Collectivité, des investigations informatiques peuvent devoir être menées.

Dans ce cas, l'équipe en charge de l'enquête notifie par écrit la nécessité de procéder à des investigations informatiques au RSSI et au Directeur de la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques, et informe le DPD des besoins d'accès aux données des utilisateurs concernés.

Toutefois, en cas d'enquête administrative, intéressant le RSSI, le Directeur de la Direction de l'Ingénierie Informatique, des Télécommunications et des Usages Numériques ou le DPD, cette notification ne sera pas effectuée.

12. PORTEE DE LA CHARTE

La présente charte revêt une portée juridique, conférant aux utilisateurs des droits et des obligations. Tout comportement répréhensible de la part d'un utilisateur peut engager la responsabilité civile ou pénale de la collectivité, en l'occurrence la Collectivité. Les infractions aux règles définies par cette charte peuvent également engager la responsabilité personnelle de l'utilisateur et entraîner des sanctions, telles que la restriction d'accès au système d'information ou des mesures disciplinaires.

La Collectivité se réserve le droit d'engager ou de faire engager des poursuites administratives, indépendamment des sanctions disciplinaires, en cas de fraude informatique, de non-respect des droits d'auteur ou de violation du secret professionnel. En cas de violation des droits de tiers, notamment en matière de propriété intellectuelle, le Directeur des Systèmes d'Information est habilité à isoler et conserver les éléments de preuve (logs, fichiers, programmes), et à signaler toute activité délictueuse aux autorités compétentes.