Copie pour impression
Réception au contrôle de légalité le 17/12/2025 à 19h03
Réference de l'AR : 008-240800821-20251210-2025_12_232-DE
Publié le 17/12/2025 ; Rendu exécutoire le 17/12/2025

Communauté de Communes ARDENNE rives de meuse

CHARTE DE LA COMMUNAUTÉ DE COMMUNES ARDENNE RIVES DE MEUSE (CCARM)

POUR LE BON USAGE

DE L'INFORMATIQUE,

DES RÉSEAUX

ET DU TÉLÉPHONE

Version initiale approuvée par le CT du 07/05/2020

Version mise à jour approuvée par CST du 20/06/2024

Version du 03/12/2025 proposée pour modification au Conseil de Communauté du 10/12/2025

SOMMAIRE :

ARTICLE 1 - PRÉAMBULE

La présente charte rappelle les règles d'utilisation des moyens informatiques et téléphoniques de la CCARM afin de favoriser un usage optimal de ces ressources en termes de sécurité, de confidentialité, de performance, de respect de la réglementation et des personnes. Elle rappelle à ses utilisateurs les droits et les responsabilités qui leurs incombent dans l'utilisation du système d'information.
Ce règlement s'applique à l'ensemble des agents, tous statuts confondus, aux élus, stagiaires, visiteurs, et plus généralement à tous les utilisateurs des moyens informatiques et téléphoniques de la Communauté.

ARTICLE 2 - DÉFINITIONS

On désignera de façon générale sous le terme « moyens informatiques », les ressources informatiques de calcul ou de gestion locales, ainsi que celles auxquelles il est possible d'accéder à distance, directement ou en cascade, à partir du réseau administré ou utilisé par la Communauté.
On désignera par « moyens téléphoniques », tous les téléphones fixes ou portables, radiotéléphones, assistants personnels, fax, modems mis à disposition par la Communauté pour l'exercice de l'activité professionnelle.
On désignera par « services Internet/Intranet », la mise à disposition par des serveurs locaux ou distants, de moyens d'échanges et d'informations diverses : site web, messagerie, forum…
L'activité professionnelle est celle qui est nécessaire, utile, dépendante ou complémentaire à l'activité des services communautaires, quelle qu'en soit la nature.

Les moyens informatiques et de télécommunications mis à disposition sont, de façon non exhaustive :

- le poste de travail : PC, portable, imprimantes, scanners, …
- les équipements nomades (notamment dans le cadre du télétravail) ;
- les espaces de stockage individuel ;
- les réseaux locaux ;
- les conditions d'utilisation des dispositifs personnels ;
- Internet ;
- la messagerie électronique ;
- la téléphonie, smartphone, portable, fax,

Les conditions d'administration du système d'information, passent notamment par :

- le système automatique de filtrage ;
- le système automatique de traçabilité ;
- la gestion du poste de travail.

ARTICLE 3 - ACCÈS AUX RESSOURCES INFORMATIQUES, SERVICES INTERNET / INTRANET ET MOYENS TÉLÉPHONIQUES

3.1 UTILISATION DES RESSOURCES :

Les ressources informatiques, l'usage des services Internet/Intranet et du réseau pour y accéder, ainsi que les moyens téléphoniques, sont mis à disposition des utilisateurs, tels que définis à l'article 5 de la présente charte, pour l'exercice des activités de la CCARM ou des services offerts à la population, voire des prestations demandées par la Communauté à ses prestataires, même occasionnels (ex : stagiaires, saisonniers).
Toutefois, il est admis qu'un usage raisonnable des ressources à des fins personnelles peut être toléré, à la condition expresse de respecter les dispositions de la présente charte. Cet usage personnel des ressources ne pourra être qu'occasionnel et limité, dans le temps et par son objet.

3.2 DOCUMENTS PRIVÉS ET PROFESSIONNELS :

L'utilisateur veillera à distinguer clairement les documents, courriers, messages, etc. qu'il considère comme personnels, des documents professionnels, notamment en les rangeant dans des dossiers distincts nommés « PRIVÉ », et/ou en faisant figurer « PRIVÉ » en tête du nom des documents et de l'objet des courriels.
Tout document ou courriel ne respectant pas cette règle sera considéré comme professionnel, donc de la propriété de la CCARM.

3.3 RESPONSABILITÉS :

L'utilisateur est informé que sa propre responsabilité, celle de son chef de service, et la responsabilité de la Communauté peuvent être engagées civilement et pénalement du fait de son comportement. Il veillera donc à respecter les lois et règlements en vigueur, notamment ceux mentionnés à l'article 6, ainsi que les règles d'utilisation, de sécurité et de bon usage décrites dans la présente charte.

3.4 ABUS ET CONTRÔLES :

L'utilisateur est informé que tout abus de l'utilisation non professionnelle pourra faire l'objet de sanctions. De ce fait, il reconnaît avoir été averti que le système d'information de la Communauté fait l'objet d'une surveillance constante (serveurs, réseaux, postes de travail, téléphones, logiciels, virus…), et qu'en cas de comportement suspect, certains équipements sont soumis à une surveillance particulière, notamment sur les volumes d'informations traitées (enregistrement, téléchargement), les durées anormales d'utilisation, les connexions à des sites internet prohibés ou les tentatives d'intrusions, par exemple.

Ainsi sont conservées de manière automatique durant une période d'un (1) an les informations suivantes :

- l'adresse (appelée URL, par exemple www.ccarm.fr) et l'heure de toute connexion à un site web depuis un ordinateur (identifié par une adresse IP telle que 157.157.123.456) utilisant le réseau de la Communauté
- une copie de tout courrier électronique réceptionné et émis par le serveur de messagerie de la Communauté, y compris les courriels non sollicités (SPAM). Pour les utilisateurs Outlook, les mails qui sont identifiés comme spam le sont sur le serveur et visibles via l'interface Webmail Icewarp, ce ne sera pas le cas non plus avec la mise en place de la solution Mailinblack, les spams ne seront visibles que via l'interface d'administration de Mailinblack.
- le numéro appelé, l'heure, la durée et le coût de tous les appels téléphoniques externes passés par les postes téléphoniques et les fax reliés au réseau téléphonique de la Communauté. Les quatre derniers chiffres sont masqués pour toute édition.
- Les logins et connexion au wifi public de la CCARM.

La gestion de ces données est faite dans le respect de la loi Informatique et Libertés, qui prévoit, pour toute personne, un droit d'accès et de rectification aux données qui la concernent, ayant fait l'objet d'un traitement informatique. L'exercice de ce droit se fait par la voie hiérarchique.

3.5 RESPECT DE LA CONFIDENTIALITE DES DONNEES :

Des utilisateurs sont amenés à gérer, du fait de leurs compétences et dans le cadre de leurs missions, des fichiers dont il est nécessaire de garantir la confidentialité : fichiers d'usagers des services, dossiers individuels et bulletins de paie des utilisateurs, etc.
Ils doivent ainsi veiller :

- à respecter l'intégrité et la confidentialité des données, tant pour la collecte, le traitement et la communication interne et externe des données,
- à ne pas copier ni sauvegarder les fichiers professionnels sur support amovible autres que ceux fournis par la collectivité,
- ne pas collecter des données qui, en raison de leur contenu, contreviendraient aux lois et règlements en vigueur.

Une gestion des droits d'accès est mise en place pour interdire l'accès aux fichiers confidentiels à toute personne autre que le ou les gestionnaires desdits fichiers.
En cohérence avec le point 3.4, l'utilisateur s'assure que son usage des outils numériques est conforme aux règles de déontologie et au respect aux règles de de probité, de secret professionnel et de discrétion professionnelle.
Il s'assure, également, que son utilisation des outils est conforme à ses missions et à ses droits d'accès. Certains utilisateurs peuvent bénéficier de droits élargis en vue de mener, ponctuellement, des interventions sur dans des outils / plateformes à la demande d'un service ou en remplacement d'un agent absent. Suivant les droits d'accès confiés, l'agent veille à ce que ses actes entrent dans le champ strict de ses missions. Tout usage

distinct des missions confiées et manifestement inhabituel ou irrégulier rompt la confidentialité des données et constitue une faute (cf. point 3.6).
L'utilisateur ne doit pas prendre connaissance d'informations attribuées à autrui sans son accord, à ne pas communiquer à un tiers de telles informations ou des informations non publiques auxquelles il peut accéder, mais dont il n'est pas propriétaire.
L'utilisateur est averti que les données enregistrées sur les serveurs partagés sont donc accessibles à d'autres utilisateurs. L'enregistrement de données à caractère personnel et confidentiel sur les serveurs partagés, sans restriction d'accès, est donc proscrit.

La protection des données personnelles informatiques
Conformément au Règlement Général à la Protection des Données (RGPD), l'utilisateur respecte l'intégrité des données (pas de modification ou suppression sans autorisation), ne diffuse pas et n'accède pas aux correspondances privées (agent-Communauté de Communes) et aux données personnelles d'agents et d'élus sauf dans le cadre strict de ses fonctions et des autorisations expressément données par sa hiérarchie.

Le RGPD accorde aux personnes physiques certains droits relatifs à leurs données personnelles qui sont :

- droit d'accès : le droit d'être informé et de demander l'accès aux données personnelles que la collectivité traite,
- droit de rectification : le droit de demander de modifier ou de mettre à jour les données personnelles lorsqu'elles sont inexactes ou incomplètes,
- droit d'effacement : le droit de demander de supprimer définitivement les données personnelles,
- droit de restriction : le droit de demander d'arrêter temporairement ou définitivement le traitement de tout ou partie des données personnelles,
- droit d'opposition : droit de refuser à tout moment le traitement des données personnelles pour des raisons personnelles, ou pour des fins de marketing direct,
- droit à la portabilité des données : le droit de demander une copie de vos données personnelles au format électronique et le droit de transmettre ces données personnelles pour une utilisation par un service tiers,

La Communauté de Communes a pris en compte ces directives.
L'utilisateur peut exercer ces droits :

- auprès du Président de la Communauté de Communes, responsable du traitement,
- ou par écrit en s'adressant au relais du Délégué à la Protection des Données (DPD) depuis la plateforme dédiée : https://www.agirhe.cdg54.fr/TDB/rgpd.aspx

Le Délégué à la Protection des Données de la Communauté de Communes est :

Centre Départemental de Gestion de la Fonction Publique Territoriale de Meurthe-et-Moselle
2, allée Pelletier Doisy 54600 VILLERS-LÈS-NANCY
Tel : 03.83.67.48.10
(Désignation CNIL n°DPO-130240)

Suivant les articles 5.2 et 24.1 du RGPD, uniquement pour une analyse post-incident (défaut technique, erreur de manipulation, usage abusif), et ce dans la limite fournie par le prestataire, les logs ou accès aux plateformes électroniques métiers (logiciels de comptabilité, d'Intranet, de Gestion Electronique des Documents (GED)) seront consultés.

Plan Vigipirate :
La divulgation d'informations confidentielles (certains plans, coordonnées etc.) ou la défaillance dans le contrôle de la confidentialité peuvent constituer des risques en matière de sécurité des biens et des personnes. Parallèlement, les attaques informatiques constituent des actes criminels voire terroristes pouvant entrainer des conséquences lourdes sur l'organisation (perte financière, atteinte à l'image, menace sur les personnes etc.).
L'utilisateur, quel qu'il soit, est sensibilisé aux bonnes pratiques numériques en particulier sur l'usage de données confidentielles, sur le risque autour de l'usurpation d'identité et les logiciels malveillants. Une veille est maintenue par le service TIC en permanence sur les éventuelles vulnérabilités des systèmes.
En cas de doutes vis-à-vis d'une demande par téléphone ou par courriel, l'utilisateur ne doit pas hésiter à en informer le service informatique ou son responsable de service.

3.6 MESURES CONSERVATOIRES ET SANCTIONS :

Tout utilisateur ne suivant pas les règles et obligations rappelées dans cette charte pourra se voir, par mesure conservatoire, suspendre l'accès aux ressources informatiques, téléphoniques, ou à certains services (internet, messagerie…).
En cas de manquement grave et d'intention manifeste de nuire au bon fonctionnement des ressources ou à l'activité des services, il sera passible de sanctions disciplinaires proportionnelles à la gravité des manquements constatés.
Tout utilisateur n'ayant pas respecté les lois pourra être poursuivi civilement et/ou pénalement.

3.7 PRISE DE MAIN ET OBSERVATION À DISTANCE :

Le service informatique dispose d'outils de prise de main à distance qui sont généralement employés pour dépanner les utilisateurs, en leur montrant directement les manipulations qu'ils ont à faire. Ces prises de main et observations à distance se feront toujours avec l'accord de l'intéressé : il est averti par un message à l'écran qu'il doit valider pour que la prise de main ou l'observation puisse démarrer.

Le service informatique dispose d'outils de prise de main à distance des serveurs. Ces prises de main et observations à distance se feront toujours avec l'accord de l'Autorité Territoriale, qu'il s'agisse de procédure de mise à jour, contrôle, sauvegarde ou d'actions de lutte et protection en cas d'attaque.
Le service informatique est ainsi doté d'une console de contrôle et d'actions à distances, dont l'usage est tracé et enregistrés.

3.8 ABSENCE DE L'AGENT :

En cas d'absence de l'agent, la continuité du service doit être assurée. L'agent doit veiller à ce que le service puisse accéder aux documents, logiciels et dossiers indispensables à l'activité (transmission des documents et dossiers aux collègues, ou mise à disposition dans un dossier partagé, création de comptes pour accéder aux applications, à l'exclusion de toute communication de mots de passe personnels). Si l'absence est imprévue (maladie, accident), le supérieur hiérarchique pourra demander au service informatique l'accès à l'espace de travail de l'agent.
En cas de départ définitif ou de mutation, le successeur récupère les documents de travail ainsi que les messages d'ordre professionnel, à l'exception des documents et messages privés (voir paragraphe Documents privés et professionnels).

ARTICLE 4 - RÈGLES D'UTILISATION, DE SÉCURITÉ ET DE BON USAGE

Tout utilisateur est responsable du bon usage des équipements mis à sa disposition. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale.
L'utilisation de ces ressources doit être rationnelle et loyale afin d'éviter leur saturation ou leur détournement à des fins personnelles.

En particulier, l'utilisateur doit appliquer les recommandations suivantes :

4.1 SECURITÉ DES DONNÉES ET DU RÉSEAU

4.1.1 Mots de passe :

Il convient de s'identifier clairement et utiliser des mots de passe pour protéger l'accès à ses matériels et programmes.
Ces mots de passe ne doivent pas être communiqués ni notés sur des supports accessibles à autrui. Ils ne doivent pas être faciles à deviner par une personne mal intentionnée (pas de prénoms ou dates de naissance de proches, par exemple). Ils doivent, obligatoirement, comporter au moins 12 caractères minimum, et doivent être changés plusieurs fois par an, en évitant de reprendre ceux qui ont déjà été utilisés.
Pour des raisons de sécurité, le service informatique se réserve le droit d'imposer le nombre de caractères minimum (12) et un changement régulier des mots de passe, GED et Intranet inclus.
Le service informatique tient à disposition des agents des moyens de générer des mots de passe sécurisés aléatoires, proposé à chaque agent.

Les mots de passe sont personnels et chaque utilisateur est responsable de l'utilisation qui peut en être faite. Ils ne doivent pas être visibles de tous. L'emploi de mots de passe communs à plusieurs personnes est interdit. Néanmoins, cette disposition ne s'applique pas lorsque les comptes ou les ordinateurs sont liés à une fonction ou à une structure (exemple : messagerie d'un service, guichet).
Seules les personnes du service informatique peuvent exceptionnellement être amenées à utiliser un mot de passe d'un utilisateur, avec son accord, pour résoudre un problème que ce dernier leur aura signalé. Une fois le problème définitivement résolu par le service informatique, l'utilisateur sera invité à modifier son mot de passe.
L'utilisateur ne communiquera aucun mot de passe au téléphone s'il n'est pas absolument sûr de l'identité et de l'habilitation de son interlocuteur. En cas de doute, il devra rappeler la personne au service informatique (numéro interne), pour poursuivre l'opération (cf. point 3.5 volet pan Vigipirate).

4.1.2 Usurpation d'identité :
Ne pas tenter de masquer sa véritable identité ou d'usurper l'identité d'une autre personne pour essayer d'accéder à ses informations ou ses traitements.
Les courriels nominatifs sont notamment protégés par le secret de la correspondance, à l'exception des courriels protocolaires et de contact (nom de service, pôle, fonction @ardennerivesdemeuse.com) lesquels ne sont pas soumis à cette protection interne.
Ainsi, concernant les mails nominatifs, nul ne peut en prendre connaissance sans autorisation de l'émetteur ou du destinataire, à l'exception d'un juge d'instruction ou d'un officier de police judiciaire, qui peut, en cas de plainte, procéder à la saisie des données nécessaires à la manifestation de la vérité.
Il convient de signaler au service informatique toute tentative d'accès anormal à son poste de travail et, de façon générale, toute anomalie que l'on peut constater (cf. point 3.5 volet pan Vigipirate).

4.1.3 Données d'autrui :
Ne pas tenter de lire, modifier, copier ou détruire des données autres que les siennes. En particulier, ne pas modifier de fichiers contenant des informations comptables ou d'identification, ni tenter de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées, exception faite des données diffusées dans des dossiers publics ou partagés qui sont clairement identifiés.
Il est expressément rappelé qu'accéder sans autorisation à des informations d'autres utilisateurs, les copier, les divulguer, les modifier ou les effacer, peut être sanctionné pénalement.

4.1.4 Informations confidentielles – déclarations CNIL :
Ne pas divulguer d'informations confidentielles, notamment par téléphone, à des tiers qui ne doivent pas les connaître. En particulier, les traitements ou fichiers concernant des informations relatives à des personnes (nom, numéro...) doivent être déclarés à la CNIL, s'ils ne sont pas expressément dispensés de déclaration. Les déclarations stipulent notamment les finalités exactes des traitements, la liste des destinataires des diverses informations, ainsi que leur durée de conservation.
Le service informatique vous assiste dans l'établissement de ces déclarations.

Les fichiers non automatisés (papier) dont les informations proviennent ou sont appelées à être enregistrées dans ces traitements, sont soumis aux mêmes contraintes, et doivent donc être utilisés avec les mêmes précautions.

Chaque utilisateur s'engage, conformément aux articles 121 et 122 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles il a accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

4.1.5 Accès aux postes de travail :

Ne pas laisser des ressources ou services accessibles à des tiers en cas d'absence du poste de travail ; se déconnecter puis mettre l'ordinateur en veille ou verrouiller le poste avant de s'absenter, même momentanément.
La mise en fonction automatique de l'économiseur d'écran, au bout de quelques minutes d'inactivité, est vivement recommandée, avec saisie obligatoire d'un mot de passe pour quitter la veille.
Restreindre l'accès aux locaux accueillant les traitements sensibles, notamment ceux soumis à déclaration à la CNIL. Veiller à ce que les impressions ou sauvegardes contenant des informations sensibles ou nominatives (noms, adresses, photos de personnes…) ne soient pas accessibles à des personnes non autorisées (conservation obligatoire sous clé dans les bureaux recevant du public). Également, tout support (papier, CDROM…) doit être rendu illisible avant mise au rebut.

4.1.6 Accès aux données et plan de classement :

4.1.6.1 Accès aux données

Ne pas laisser des ressources ou services accessibles à des tiers en cas d'absence du poste de travail ; se déconnecter puis mettre l'ordinateur en veille ou verrouiller le poste avant de s'absenter, même momentanément.

4.1.6.2 Plan de classement

Chaque serveur affecté à un service respecte un plan de classement préalablement déterminé et admis des utilisateurs. A cette arborescence, s'applique le respect de la hiérarchie des données et des procédures de sauvegarde ad'hoc.
Les documents intermédiaires, provisoires, les différentes versions menant à une rédaction définitive sont secondaires, et devront être distincts dans le plan de classement du dossier définitif.
Les fichiers au fil de l'eau, ne peuvent être concernés par cette notion. Ils seront sauvegardés selon la procédure générale.
Les documents ou fichiers ouverts à des personnes temporairement admises à travailler sur le réseau : stagiaire, saisonnier, renfort, seront dotés d'un ordinateur aux droits restreints. Un dossier générique sera créé pour tous

services appelés trash, dans lequel seront regroupés les dossiers et fichiers superflu, lesquels seront sauvegardés sur un support externe avant d'être effacés une fois par an.
Le plan de classement à deux objectifs :

- Accéder facilement aux données selon leur importance et contenu,
- Ne pas saturer les serveurs inutilement de données obsolètes, inutiles, secondaires voir superflues.

4.1.7 Sauvegardes :

4.1.7.1 Procédures

Quelle que soit la qualité des moyens de défense mis en œuvre (physique ou logiques), les données peuvent être altérées sciemment ou accidentellement. Les données et les applications informatiques doivent être disponibles « à tout moment » lorsqu'on en a besoin, et doivent être conservées (sauvegardées) afin de pouvoir être récupérées (restauration) le moment voulu. Il convient par conséquent de :

- Définir une politique de sauvegarde ;
- Définir des procédures de sauvegarde ;
- Définir des procédures de restauration ;
- Maintenir ces politiques et procédures.

Les utilisateurs ont connaissance de leur existence, mais non de leur contenu.
Ainsi, toutes autres formes de sauvegarde n'est pas autorisée.
À de rare exception, elle pourrait être programmée, sur des supports externes mis à la disposition de la Communauté, en lien avec le service informatique.
La sauvegarde de fichiers professionnels sur des sites extérieurs (cloud, outils google, …), ou par envoi sur des adresses courriels personnelles n'est pas autorisée.

4.1.7.2 Plan de sauvegarde

Le plan de sauvegarde intègre les éléments suivants :

- Le périmètre (liste des ressources à sauvegarder) ;
- Les différents types de sauvegarde ;
- La fréquence des sauvegardes ;
- La procédure d'administration, d'exécution des sauvegardes et vérification régulière de la bonne réalisation ;
- Les informations de stockage et les restrictions d'accès aux sauvegardes ;
- Les procédures de test de restauration ;
- La destruction des supports ayant contenu les sauvegardes.

Ce plan doit être mis à jour à chaque déploiement de nouveau système ou application. L'ensemble des opérations de sauvegarde est journalisé. Les journaux sont conservés avec les supports de sauvegardes

Les utilisateurs ont connaissance de son existence, mais non de son contenu.

4.1.8 Téléchargement et installation de logiciels :

Ne pas télécharger, installer, utiliser ou contourner les restrictions d'utilisation d'un logiciel pour lequel la Communauté n'a pas acquis de licence. Seules les personnes du service informatique sont habilitées à installer des logiciels, y compris des logiciels libres, et utilisent pour cela des comptes d'administrateurs sur les machines. Les autres utilisateurs disposent de comptes d'utilisation restreints qui sont suffisants pour un usage courant.

Tous les logiciels doivent faire l'objet d'une demande officielle d'installation au service informatique qui en définira les modalités.

4.1.9 Téléchargement de mises à jour :

Par défaut, ne pas télécharger, installer, ouvrir de fichier de mise à jour de logiciels ou application dont on n'est pas absolument certain de la provenance et de l'innocuité. Seules les personnes du service informatique sont habilitées à certifier les mises à jour obligatoires, nécessaires et sûres.

4.1.10 Droits de reproduction :

Ne pas copier un logiciel pour l'utiliser sur un autre poste, ou en dehors de son lieu de travail. Les copies de sauvegarde de logiciels, prévues par le code de la propriété intellectuelle, sont exclusivement effectuées par le service informatique, sauf dans le cas de l'acquisition directe d'un logiciel par un autre service.

Des droits de reproduction existent également pour les œuvres littéraires, musicales, photographiques, audiovisuelles, qui ne doivent en aucun cas être téléchargées sur internet, reproduites ou diffusées sans autorisation de l'auteur, ou du propriétaire des droits d'exploitation.

4.1.11 Photographies, droit à l'image :

L'image d'une personne ne peut être utilisée ou diffusée sans son consentement écrit (celui de son responsable légal pour un mineur). D'une manière générale, les photos que les agents peuvent être amenés à prendre dans l'exercice de leurs fonctions ne doivent donc pas comporter de personnes, plaques d'immatriculation, enseignes de magasins étrangères à l'affaire : il est recommandé de flouter ces éléments.

Les photos prises dans le cadre des activités de la Communauté ou dans ses locaux ne peuvent pas être utilisées à des fins personnelles, et sont interdites à la diffusion externe sans le consentement écrit de la Direction Générale.

Cette recommandation s'applique aux enregistrements vidéo et sonores.

4.1.12 Équipements étrangers :

Ne pas connecter sans autorisation, à un poste ou au réseau, un équipement étranger à la Communauté (disques durs externes, clé USB, modems, téléphones et smartphones…) et susceptible de provoquer des dysfonctionnements, ou d'introduire des virus informatiques.

Toute connexion d'un nouveau matériel doit se faire avec l'autorisation préalable du service informatique et nécessitera un scan du support sur le poste concerné sans ouverture des fichiers avant la fin de l'analyse de l'antivirus.

Ainsi, considérant que certaines conditions seraient de nature à tolérer la connexion de matériel extérieur : formation, conférence, présentation, …, la connexion se fera après un scan du support sur le poste concerné sans ouverture des fichiers avant la fin de l'analyse de l'antivirus. (Se reporter également, pour information, aux points 4.1.15 / 4.1.16 / 4.1.17 / 4.1.19 / 4.1.21).

Les agents amenés à être placés potentiellement en travail nomade ne peuvent pas utiliser leur propre matériel informatique. Sont utilisables, soit l'ordinateur portable lié à leur poste de travail ou le prêt d'un ordinateur portable par le service informatique de la Communauté de Communes. Dans ce cadre, aucun équipement étranger ne pourra y être connecté (smartphone, clé USB personnelle...). La qualité du réseau pourra être évaluée par le service TIC sur demande.

4.1.13 Messagerie :

Ne pas ouvrir de pièce jointe d'un courriel dont on n'est pas absolument certain de la provenance et de l'innocuité. Si cette pièce jointe est un document contenant des macros (tels que Word ou Excel), ne pas permettre l'exécution de ces macros dans ce cas. Il est possible que des actions préjudiciables soient effectuées par ces macros (macrovirus).

La messagerie dispose d'un outil de filtrage qui élimine automatiquement tout message suspect, en entrée et en sortie. La sélection est faite sur le type et le nom des pièces jointes. Sont également éliminés tous les messages considérés comme des « pourriels » (spam), et qui sont reconnus par la teneur du titre ou du texte du message (recherche de termes tels que viagra…). Attention, ces filtres ne sont pas fiables à 100%. Certains pourriels ne sont pas détectés, et il peut aussi arriver que des messages légitimes soient écartés. Si vous avez des raisons de penser qu'un message vous étant destiné a été éliminé, adressez-vous au service informatique qui pourra effectuer des vérifications.

Actuellement les mails sortants ne sont conservés que dans les archives Outlook, il n'y a pas de copies sur le serveur. Si le message est effacé sur le serveur il sera automatiquement effacé dans Outlook et vice versa

L'utilisation, à titre professionnel, de comptes de messagerie non gérés par la CCARM est interdite. Les comptes professionnels se terminent obligatoirement en @ardennerivesdemeuse.com

▲ Remarque importante :

Un message électronique peut constituer une preuve, et peut engager fermement son expéditeur et son destinataire : il existe un risque réel pour qu'un agent prenne des engagements qu'il faudra ensuite respecter. Toutes les recommandations concernant les échanges écrits avec des tiers s'appliquent donc à la messagerie. L'envoi de messages électroniques doit respecter les mêmes procédures de contrôle, de validation, d'autorisation que les courriers.

Il est souhaitable de mettre systématiquement en copie des messages importants, son responsable et le responsable du destinataire, et il est obligatoire de transmettre pour validation à un responsable tout message

qui aurait valeur contractuelle ou d'engagement. Pour autant, cette copie, ne vaut pas visa, n'a vocation que d'information, la validation est impérative et doit être opposable pour couvrir l'agent. Si la décision, ou transmission, nécessite un niveau d'accréditation supérieur, c'est au n+1 de faire remonter la demande de validation, bon pour transmission.
Dans certain cas, il sera préférable de privilégier un envoi depuis la boite de president@ardennerivesdemeuse.com, après validation de l'Autorité Territoriale et ou son représentant par délégation.
Par ailleurs, tout message important doit être conservé à des fins d'archivage.

4.1.13.1 Les adresses nominatives

La CCARM a autorisé la création de courriel au nom des agents. Pour rappel, ces courriels nominatifs sont protégés par le secret de la correspondance. En cela, ils ne sont pas de la propriété de la CCARM, cependant, l'échange de données avec l'extérieur, impliquant la Communauté, donc sa responsabilité, nécessite plusieurs mises en garde.
La sauvegarde des fichiers Outlook des courriels nominatifs se fera sur autorisation expresse de l'utilisateur.
La sauvegarde se fera sur le serveur de sauvegarde. Les courriels seront conservés un an sur le serveur de messagerie, puis détruit, pour libérer de la place. L'accès aux anciens courriels se fera sur demande, par consultation de la sauvegarde, lorsque celle-ci aura été autorisé par l'agent.
Au départ de la Communauté, les mails sauvegardés seront détruits.
La Communauté ne sauvegardera pas les fichiers Outlook locaux, c'est-à-dire sur le disque dur du PC.
Pour rappel, même si les courriels sont protégés, les données échangées ne peuvent être de la propriété de la Communauté.

4.1.13.2 Les adresses protocolaires (professionnelles)

Il s'agit des adresses de contact et d'échanges avec l'extérieur, consultable par quiconque du service y est autorisé. Ainsi aucun échange de nature personnelle ne peut transiter par ces adresses.
La sauvegarde et le nettoyage annuel sont systématiques, de même que les opérations de suppression du serveur courriel.
À la différence des courriels nominatifs, il n'y a pas de durée de conservation limitée de ces fichiers.

4.1.14 L'intranet de la Communauté

L'intranet est un site réservé aux agents de la Communauté. Le système est accessible depuis l'intérieur, comme de l'extérieur. C'est un réseau privé de la CCARM qui permet de mettre en commun les ressources de la Communauté comme des contacts, ou tout simplement dématérialiser des procédures ou des documents comme : des informations, des services, des procédures, des outils, des documents personnels à télécharger (arrêtés, …), etc
L'accès aux différents modules est paramétré et adapté selon le service d'affectation de l'agent. À terme, les élus pourraient y accéder.
Un certificat, installé par nos informaticiens, permet la protection de ce site lors de son accès par l'extérieur de la Communauté.

L'intranet de la Communauté permet aux agents habilités d'accéder à la gestion des messages déposés par les administrés sur la plateforme de Saisine par Voie Electronique (SVE).

▲ Remarque importante :
Un message électronique sur la plateforme « SVE » peut constituer une preuve, et peut engager fermement son expéditeur et son destinataire : il existe un risque réel pour qu'un agent prenne des engagements qu'il faudra ensuite respecter. Toutes les recommandations concernant les échanges écrits avec des tiers s'appliquent donc à cette plateforme. L'envoi de messages doit respecter les mêmes procédures de contrôle, de validation, d'autorisation que les courriers.
Il est obligatoire de transmettre pour validation à un responsable tout message qui aurait valeur contractuelle ou d'engagement. La validation est impérative et doit être opposable pour couvrir l'agent. Si la décision, ou transmission, nécessite un niveau d'accréditation supérieur, c'est au n+1 de faire remonter la demande de validation, bon pour transmission.
Dans certain cas, il sera préférable de privilégier un envoi depuis la boite de president@ardennerivesdemeuse.com, après validation de l'Autorité Territoriale et ou son représentant par délégation ou au minimum depuis une boite protocolaire.

Tous les messages sur cette plateforme « SVE » sont conservés suivant les règles posées par le RGPD. Leur valeur confidentielle bénéficie des mêmes prescriptions posées au point 3.5.

4.1.15 Virus :
L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux, que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques…
Des comportements inhabituels d'un logiciel ou d'un ordinateur tels que l'ouverture de fenêtres intempestives, l'activité inexpliquée du disque dur ou la dégradation importante des performances peuvent traduire la présence d'un logiciel parasite : contacter rapidement le service informatique.

4.1.16 Antivirus :
Le service informatique installe sur les machines un logiciel destiné à vous protéger des programmes malveillants. Cet outil ne doit pas être désinstallé, ni désactivé, et il est paramétré pour se mettre à jour régulièrement (reconnaissance de nouveaux virus). Le paramétrage ne doit donc pas être modifié, et il est recommandé aux utilisateurs d'ordinateurs portables de se connecter régulièrement au réseau informatique pour que cette mise à jour puisse être effectuée.
Attention, en cas de détection de virus, un message du logiciel antivirus vous avertit : veuillez contacter immédiatement le service informatique.

4.1.17 Protection de la messagerie
La Communauté a fait le choix de souscrire à la solution Mailinblack Protect, conçue pour détecter les spams, newsletters indésirables et virus et trier automatiquement notre messagerie. En effet les mails sont pour plus

de 90% à ce jour, le moyen de cyberattaques via un ransomware, malware ou tentative de phishing, ayant pour effet, la dégradation, le vol de données, ou encore des dommages financiers. La solution consiste à mettre un filtre entre le serveur de messagerie et les adresses mails afin de reconnaitre les mails autorisés, préalablement identifiés.
En aucun cas les utilisateurs ne devront contourner cette solution par la transmission d'adresse de contact extérieure au nom de domaine de la Communauté.

4.1.18 Le transfert de documents depuis une plateforme en ligne

Certaines messageries professionnelles ne permettent pas d'envoyer des fichiers conséquents.
Le We Transfer (Max. 20 Go) ou Swiss Transfer (Max. 50 Go) sont des services de transfert de fichier fondés sur le cloud, sécurisés en matière de protection des données. Ils permettent l'envoi gratuit de ces fichiers.
L'envoi concerne des pièces courantes. Aucune donnée confidentielle ne doit transiter sur ces plateformes.

4.1.19 Smartphone, tablette et solution nomade

Concernant ce point précis, la première barrière de sécurité est et restera toujours l'utilisateur. En effet, le matériel sortant du système de la CCARM, donc du périmètre d'actions défini par les mesures de protection, il devient difficile d'en contrôler l'usage.
Ainsi, les règles à respecter sont :

- Pour les smartphones :
  - Interdiction d'utiliser la carte SIM de la CCARM dans un autre terminal que celui fourni par la CCARM,
  - En cas de double SIM (pro et perso), les règles d'usage à appliquer sont celles de la CCARM,
  - Mise en place systématique d'un antivirus (BitDefender propose une solution) avec scan automatique programmé,
  - Interdiction d'installer des applications sans consultation du service informatique,
  - Le rechargement sur secteur est obligatoire,
  - Éviter tout transfert ou connexion aux PC,
  - Limitation de l'usage aux seules fins de la CCARM (messagerie, applications, internet), une tolérance est acceptée pour les agents et élus répondant de contraintes particulières,
  - Utilisation des applications de vérification incluses dans le système Android ou Apple (malheureusement, celles-ci variant suivant les modèles, il faudra, au service informatique, faire une procédure pour chaque modèle d'appareil),
- Pour les terminaux type portables ou tablettes :
  - Limiter l'usage aux seules fins de la CCARM (pas d'usage à titre personnel),
  - Effectuer les mises à jour dès qu'elles sont disponibles (OS et antivirus), et s'assurer que tout soit à jour avant d'utiliser le poste de travail,
  - Programmer des vérifications anti-virus approfondies chaque semaine,
  - Pour la majorité des agents : limiter l'usage à l'accès en mode web des applications : messagerie, extranet,…

- Pour les agents en travail nomade : utilisation du VPN (Virtual private network) ou RPV (Réseau privé virtuel), système permettant l'accès à une connexion réseau protégée. Ce système est installé, donc utilisable, uniquement sur le matériel informatique fourni par la Communauté de Communes.

4.1.20 Perte, vol ou accident

En cas de perte ou de vol ou d'un incident endommageant téléphone, smartphone ou PC portable appartenant à la CC et mis à disposition d'un agent ou d'un élu, ce dernier a l'obligation d'en informer sans délai la Communauté pour qu'elle puisse prendre les mesures ad hoc : opposition sur les lignes téléphoniques, dépôt de plainte, etc…

4.1.21 BYOD, ou l'utilisation d'équipements informatiques personnels dans un environnement professionnel

Ce qui est appelé "BYOD "[1] n'est aujourd'hui pas proscrit car, comme la CNL le mentionne, il s'agit d'un choix de l'employeur qui peut l'autoriser, sous conditions, ou l'interdire. Cet usage a été nécessaire lors de la crise sanitaire du COVID pour faire face au manque de matériel informatique manquant à la généralisation du télétravail.

Face à la cybercriminalité, la Communauté de Communes a dû augmenter son niveau de vigilance. La CCARM, responsable des données personnelles de la collectivité, n'autorise pas l'usage de matériel informatique personnel dans un environnement professionnel.

En ce sens, la CCARM équipe désormais l'ensemble de ses agents du matériel nécessaire à la mise en place du travail nomade.

Cependant, elle pourrait, sous certaines limites et dans un contexte de gestion de crise spécifique (contexte de déclenchement du plan ORSEC ou d'une crise sanitaire, lors de l'apparition du COVID), autoriser cet usage.

Alors, en qualité d'employeur, elle est responsable des données personnelles de la collectivité "y compris lorsqu'elles sont stockées sur des terminaux dont il n'a pas la maîtrise physique ou juridique, mais dont elle a autorisé l'utilisation pour accéder aux ressources informatiques de l'entreprise".

Considérant les implications techniques, notamment, que tout le matériel utilisé devrait faire l'objet d'une procédure : contrôle de l'accès / bulle de sécurité, chiffrement de flux, sensibilisation etc , … Considérant qu'il s'agit de matériel personnel,
Considérant la technologie nécessaire, et la responsabilité pesante sur l'agent, cet usage est limité aux applications de communication.

Concernant le respect de la vie privée, l'employeur peut avoir accès uniquement à la partie professionnelle du matériel utilisé. L'agent pourrait ainsi identifier clairement l'objet et le ou les dossiers utilisés sur un matériel privé. Cette cible permettrait d'établir la limite entre le personnel et le professionnel.

[1] Bring Your Own Device », en français : « Apportez Votre Equipement personnel de Communication » ou AVEC

Ainsi, en effet, dans la mesure où le matériel peut être certifié comme non dangereux pour le système général, la charte informatique limite l'utilisation de matériel personnel (ordinateur, tablette et téléphone portable) dans le cadre professionnel en respect de la vie privée et de la protection des données professionnelles, la consultation et l'envoi de mails, sms,…, nécessaires à l'activité à distance.

Le BYOD n'est pas imposé aux agents non dotés de moyens, par la Communauté.

4.2 RÈGLES MINIMALES DE COURTOISIE ET DE RESPECT D'AUTRUI

Il convient de faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques (courriels, forums de discussions…).

4.2.1 Opinions personnelles et propos illicites :

Ne pas émettre d'opinions personnelles étrangères à son activité professionnelle, et susceptibles de porter préjudice à la Communauté. Sont notamment interdits la consultation, la rédaction, le téléchargement, l'enregistrement, l'envoi et la diffusion de messages, textes, images, films, pages web, etc. à caractère injurieux, raciste, antisémite, discriminatoire, insultant, dénigrant, diffamatoire, dégradant, pornographique, faisant l'apologie de crime, incitant à la haine…

De même, les propos susceptibles de révéler les opinions politiques, religieuses, philosophiques, les mœurs, la santé des personnes, ou encore de porter atteinte à leur vie privée ou à leur dignité, ainsi que les messages portant atteinte à l'image, la réputation ou à la considération de la CCARM sont à proscrire.

▲ Remarque : un agent ne peut être tenu pour responsable s'il reçoit de tels documents sans les avoir sollicités, mais il lui est demandé de les détruire sans délai.

4.2.2 Messages non sollicités :

Veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés, afin d'éviter l'encombrement inutile de la messagerie et une dégradation des temps de réponse. Attention, les messages non sollicités (appels à la solidarité et autres chaînes) que leur auteur demande de diffuser à un maximum de personnes, sont généralement des canulars. En cas de doute, le service informatique pourra vous conseiller au mieux.

4.2.3 Emploi de la langue Française :

Éviter l'emploi de termes en langue étrangère dans des courriers ou communications. Lorsque des termes français de même sens existent, leur emploi est obligatoire.

ARTICLE 5 - APPLICATION DE LA CHARTE

La présente charte s'applique à l'ensemble des agents de la CCARM, tous statuts confondus, aux élus, stagiaires, visiteurs, et plus généralement à l'ensemble des personnes, permanentes ou temporaires, utilisant les moyens informatiques et téléphoniques de la CCARM.

Elle fera l'objet d'une large diffusion, tant collective qu'individuelle, par tout moyen utile (intranet (en cours d'élaboration), parapheur, messagerie, note de service, affichage…) afin que nul ne puisse en ignorer son existence et son contenu.
Ainsi, dès l'entrée en vigueur de la présente charte, et la mise en œuvre de l'intranet, chaque personne concernée et visée au présent article aura accès au texte de la version en vigueur, notamment sur l'intranet, à la rubrique « charte ». Elle devra en prendre immédiatement connaissance et sera tenue sans délai au respect des règles qui y sont édictées.
La présente version de la charte est répertoriée sous le numéro indiqué en pied de page, et a été soumise à l'appréciation du Comité Social Territorial du 20 juin 2024.
Chaque nouvelle version sera validée et diffusée de la même manière. La version en vigueur sera la plus récente.

ARTICLE 6 – INFORMATIONS FORMATIONS

La CCARM fera la publicité de la charte informatique, par voie d'affichage, disponible sur l'intranet et son annexion au règlement intérieur.
En cas de doute, il est recommandé à chaque agent de contacter le service informatique pour toute question relative à la sécurité du système d'information, du matériel mis à sa disposition ainsi que du niveau de sureté de celui-ci.
La CCARM organisera des actions régulières de sensibilisation et de formation aux règles de sécurité interne à destination des agents et élus. Le service des Ressources Humaines s'assurera de diffuser les informations relatives à ces sessions.

ARTICLE 7 - BASES LÉGALES

Le présent article a pour objectif d'informer les utilisateurs des principaux textes législatifs et réglementaires définissant notamment les droits et obligations des personnes utilisant les moyens informatiques. Il ne s'agit en aucune manière d'une liste exhaustive.
Loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n°84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale, imposant notamment les obligations de réserve, de discrétion et de secret professionnel des agents publics.

Loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

Loi n°78-17 du 6 janvier 1978, modifiée, relative à l'informatique, aux fichiers et aux libertés, qui a notamment pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique et d'encadrer l'utilisation des données à caractère personnel dans les traitements informatiques.

Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.
Code Pénal, pris notamment en ses articles 323-1 à 323-7 visant les atteintes aux systèmes de traitement automatisé des données.

Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

L'ordonnance N° 2005-1516 du 8 décembre 2005, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, permet notamment à une administration de répondre par voie électronique à une demande d'information d'un usager ou d'une autre administration qui lui a été adressée par la même voie, et prévoit que les actes des administrations peuvent être signés électroniquement pour assurer l'identification du signataire et l'intégrité des actes.

Code de la Propriété Intellectuelle. Il reconnaît les logiciels comme œuvres de l'esprit, et à ce titre, ils sont protégés sans nécessiter de dépôt ou d'enregistrement.

Code du Patrimoine, pris notamment en ses articles L211-1 à L211-4. Il définit les archives comme étant l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité. Les archives publiques sont notamment les documents qui procèdent de l'activité des collectivités territoriales.

Loi n°94-665 du 4 août 1994 modifiée, relative à l'emploi de la langue française. Elle prévoit, lorsqu'ils existent, l'emploi de termes français de même sens en lieu et place des termes étrangers... .

La loi n° 2018-493 du 20 juin 2018 est venue modifier la loi Informatique et Libertés afin de mettre en conformité le droit français avec le cadre juridique européen. Les dispositions du RGPD et de la directive 2016/680 ont été codifiées par ordonnance et intégrées dans la loi du 6 janvier 1978, de manière à offrir un cadre juridique clair.