

EXTRAIT DU REGISTRE DES DÉLIBÉRATIONS
DU CONSEIL SYNDICAL

SIVOM LA GRAVE VILLAR D'ARENE

Séance du 18 juin 2026

Objet de la délibération
Charte informatique

Numéro de la délibération
N° 28.2026

Date de la convocation
27 mai 2026

Date d'affichage
22 juin 2026

L'an deux mille vingt-six, et le dix-huit juin à 18h00,

Le Conseil Syndical du SIVOM de la Grave – Villar d'Arène, dûment convoqué le vingt-sept mai deux mille vingt-six, s'est réuni au nombre prescrit par la loi, dans le lieu habituel de ses réunions, une réunion en session ordinaire, sous la présidence de Madame Béatrice ALBERT, Vice-Présidente.

Présents : Béatrice ALBERT, Julie ARNAUD, Stéphane FERRIER, Monique GIRARD, Alex DA SILVA VIEIRA

Pouvoir : de Philippe SIONNET à Stéphane FERRIER

Nombre de membres en exercice : 6

Nombre de membres présents : 5

Nombre de pouvoir : 1

Nombre de votants : 6

Le quorum (4) est atteint (5 présents + pouvoir)

Secrétaire de séance : Julie ARNAUD

*** * ***

VU le Code général des collectivités territoriales ;

VU le règlement général sur la protection des données (RGPD) du 27 avril 2016 applicable depuis le 25 mai 2018 ;

VU les obligations de la collectivité en matière de sécurité des systèmes d'information et de protection des données personnelles ;

VU la nécessité d'encadrer l'utilisation des outils informatiques et numériques mis à disposition des agents et des élus de la collectivité ;

VU l'avis favorable du comité social territorial en date du 30 avril 2026 ;

CONSIDÉRANT que le SIVOM met à disposition des agents et des élus des équipements informatiques, des outils numériques et un accès aux réseaux de communication ;

CONSIDÉRANT qu'il appartient à la collectivité de définir les conditions d'utilisation de ces moyens afin d'en garantir la sécurité, la confidentialité et le bon fonctionnement ;

CONSIDÉRANT la nécessité de prévenir les risques liés à l'utilisation des systèmes d'information, notamment en matière de cybersécurité, de protection des données et de responsabilité juridique ;

CONSIDÉRANT que la mise en place d'une charte informatique permet de sensibiliser les utilisateurs aux bonnes pratiques et de formaliser les droits et obligations de chacun ;

AR Prefecture

005-240500264-20260618-28_2026-DE
Reçu le 22/06/2026

Délibération n°28.2026 – Charte informatique

La présente délibération peut faire l'objet d'un recours contentieux devant le tribunal administratif dans un délai de deux mois à compter de sa publication/notification.

La Vice-Présidente **PROPOSE**, la charte information en annexe de la délibération.

Le Conseil Syndical, après en avoir délibéré :

DÉCIDE

- d'approuver la mise en place d'une charte informatique au sein du SIVOM, jointe en annexe à la présente délibération ;
- de préciser que cette charte s'applique à l'ensemble des agents, élus et toute personne amenée à utiliser les systèmes d'information de la collectivité ;
- que la charte sera portée à la connaissance de l'ensemble des utilisateurs et intégrée au règlement intérieur ;
- de charger Monsieur le Président de veiller à l'exécution de la présente délibération ;

Nombre de voix pour : 6

Nombre de voix contre : 0

Nombre d'abstentions : 0

Nombre de déports : 0

Ainsi fait et délibéré en séance, les jours, mois et an susdits.

La Vice-Présidente,
Béatrice ALBERT



La secrétaire de séance,
Julie ARNAUD

AR Prefecture

005-240500264-20260618-28_2026-DE
Reçu le 22/06/2026

Délibération n°28.2026 – Charte informatique

La présente délibération peut faire l'objet d'un recours contentieux devant le tribunal administratif dans un délai de deux mois à compter de sa publication/notification.



SIVOM LA GRAVE – VILLAR D'ARENE

RÉPUBLIQUE FRANÇAISE LIBERTÉ – ÉGALITÉ - FRATERNITÉ

DÉPARTEMENT DES HAUTES-ALPES
ARRONDISSEMENT DE BRIANÇON
CANTON DE BRIANÇON 1



CHARTRE DE BON USAGE DES MOYENS INFORMATIQUE ET DE TELECOMMUNICATION

**Pour le SIVOM de la Grave – Villar d'Arène,
la mairie de la Grave et la mairie de Villar d'Arène**

AR Prefecture

005-240500264-20260618-28_2026-DE
Reçu le 22/06/2026

PRÉAMBULE :

Le développement des technologies de l'information et de la communication a conduit les agents et les élus du **SIVOM de La Grave – Villar d'Arène** à recourir, dans le cadre de leurs activités professionnelles, aux outils informatiques, aux réseaux et aux services de communication numérique nécessaires à l'exécution de leurs missions.

L'utilisation de ces moyens peut comporter un certain nombre de risques, tant d'ordre technique que juridique, susceptibles d'engager la responsabilité de la collectivité ainsi que celle de ses agents et élus.

La présente charte a pour objet de sensibiliser les utilisateurs aux risques liés à l'usage de ces ressources, notamment en matière d'intégrité et de confidentialité des informations traitées.

Ces risques impliquent le respect de règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet entraîner des conséquences graves, de nature à engager sa responsabilité civile et/ou pénale.

La présente charte, qui se veut avant tout **un document d'information et de référence**, a ainsi pour objectifs :

- De déterminer les conditions d'utilisation des moyens et/ou ressources informatiques mis à disposition ;
- De définir les droits et obligations des utilisateurs de ces outils, dans le respect des droits et libertés de chacun ;
- D'informer et de sensibiliser aux risques encourus afin de les prévenir et de garantir la sécurité, l'intégrité et la confidentialité des données.

La présente charte est susceptible d'être modifiée afin de tenir compte des évolutions technologiques, organisationnelles et réglementaires, le cas échéant.

Chaque utilisateur s'engage à en respecter les dispositions.

AR Prefecture

005-240500264-20260618-28_2026-DE
Reçu le 22/06/2026

SOMMAIRE :

1. Outils mis à disposition par le SIVOM et/ou les communes	Page 4
2. Champ d'application de la charte	Page 4
2.1 Les utilisateurs concernés.....	Page 4
2.2 Les systèmes d'information et de communication.....	Page 4
3. Utilisation des matériels et des logiciels mis à disposition	Page 4
3.1 Poste informatique	Page 4
3.2 Poste de travail nomade	Page 5
3.3 Copieur multifonction.....	Page 5
3.4 Poste téléphone fixe	Page 6
3.5 Téléphone mobile	Page 6
3.6 Logiciels	Page 6
3.7 Signature électronique et certificat.....	Page 6
3.8 Messagerie électronique	Page 7
4. Moyens destinés à assurer la sécurité informatique	Page 8
4.1 Compte « utilisateur » et mot de passe	Page 8
4.2 Dispositif de prévention des virus informatique	Page 9
4.3 Prévention des risques liés à la messagerie électronique.....	Page 9
4.4 Utilisation d'internet.....	Page 9
4.5 Utilisation des réseaux sociaux.....	Page 10
4.6 Le télétravail	Page 10
5. Droits et devoirs des utilisateurs	Page 10
5.1 Principe généraux	Page 10
5.2 Respect de la confidentialité des données.....	Page 11
6. Le droit à la déconnexion	Page 11
Récépissé charte informatique.....	Page 12

AR Prefecture

005-240500264-20260618-28_2026-DE
Reçu le 22/06/2026

1. OUTILS MIS A DISPOSITION PAR LE SIVOM ET/OU LES COMMUNES :

- Poste informatique fixe
- Poste de travail nomade
- Station d'accueil (dock)
- Pack Office 365

Services et logiciels :

- Service managé « Ninja »
- Logiciel métier
- NAS / Tank'r

Accès et connectivité :

- VPN

Téléphonie :

- Téléphone fixe
- Téléphone mobile

2. CHAMP D'APPLICATION DE LA CHARTE :

2.1 Les utilisateurs concernés

La présente charte s'applique à toute personne ayant un lien statutaire ou contractuel avec la collectivité, ainsi qu'aux élus et au prestataire informatique, dès lors qu'elle utilise les outils informatiques mis à disposition pour l'exécution de ses missions.

À noter : les stagiaires et les saisonniers utilisant ces moyens doivent également se présenter au bureau du SIVOM afin de signer cette charte avant toute utilisation.

2.2 Les systèmes d'information et de communication

Les systèmes d'information et de communication incluent l'ensemble des équipements informatiques et électroniques de la collectivité, qu'ils soient interconnectés ou non. Cela comprend notamment :

- Les ordinateurs (fixes ou portables)
- Les périphériques et réseaux informatiques (NAS, Tank'r, VPN...)
- Les photocopieurs, télécopieurs, imprimantes et scanners
- Les téléphones fixes et mobiles
- Les logiciels, fichiers, données et bases de données
- Les systèmes de messagerie
- Les connexions Internet, intranet et extranet

3. UTILISATION DES MATÉRIELS ET DES LOGICIELS MIS A DISPOSITION :

3.1 Poste informatique :

Du matériel informatique est mis à disposition de chaque utilisateur. Ce matériel est fragile : chacun doit en prendre soin. Il comprend notamment :

- Unité centrale, écran, souris, clavier, ordinateur portable, station d'accueil
- Système d'exploitation : Windows
- Logiciels : pack bureautique, messagerie, logiciels métiers spécifiques

AR Prefecture
005-240500264-20260618-28_2026-DE
Reçu le 22/06/2026

Engagements des utilisateurs :

Tout utilisateur s'engage à ne pas :

- Modifier le fonctionnement, le paramétrage ou les caractéristiques de son poste (installation de matériel ou de logiciels, modification des fichiers système...)
- Interrompre, même temporairement, le fonctionnement de tout système connecté au réseau
- Accéder ou tenter d'accéder aux informations privées d'autres utilisateurs (ex. : utilisation d'un mot de passe tiers)
- Modifier ou détruire des informations communes partagées sur le réseau

Enregistrement et stockage des données :

- Les travaux doivent être enregistrés dans l'espace prévu à cet effet : NAS.
- Tout document stocké hors de ces répertoires pourra être supprimé par les administrateurs.
- Les données stockées localement sur les PC ne sont pas sauvegardées.
- Il est strictement interdit d'avoir des dossiers personnels sur le NAS.

3.2 Poste de travail nomade :

Les postes de travail nomades sont mis à disposition pour un usage strictement professionnel et exclusivement par les personnes ayant signé la présente charte.

Responsabilités des utilisateurs à l'extérieur des locaux :

- L'utilisateur assure la garde et la responsabilité de l'équipement lors de réunions ou interventions hors des locaux de la collectivité.
- La confidentialité et la sécurité des informations doivent être renforcées : éviter tout accès ou usage par des tiers non autorisés.
- Les mêmes obligations de sécurité et de confidentialité que sur site s'appliquent, avec les prescriptions complémentaires éventuelles.
- Il n'est pas recommandé de se connecter à des points d'accès Wi-Fi publics non sécurisés.

En cas d'incident :

- Tout dysfonctionnement, blocage, perte ou vol de l'équipement ou des données doit être immédiatement signalé à la direction.
- L'utilisateur doit collaborer avec la collectivité pour toutes démarches nécessaires : dépôt de plainte, déclaration d'assurance, déclaration à la CNIL, etc.

3.3 Copieurs multifonctions :

Les copieurs, du fait de leurs fonctionnalités étendues, constituent des périphériques dont la sécurité doit être assurée au même titre que celle des postes de travail informatiques. Dès lors que des informations sensibles ou à protéger transitent par ces appareils, l'ensemble des recommandations et réglementations relatives aux systèmes d'information s'applique.

Numérisation et traitement des documents :

- Lors de la numérisation, les utilisateurs doivent s'assurer que la destination des fichiers générés est accessible uniquement aux personnes habilitées à consulter ces informations.
- Les utilisateurs doivent s'abstenir de reproduire, copier ou diffuser des pages web, images, photographies, textes ou toute autre création protégée par le droit d'auteur.

AR Prefecture

005-240500264-20260618-28_2026-DE
Reçu le 22/06/2026

Sensibilisation à l'usage responsable de l'impression :

- Éviter l'impression systématique des mails, en particulier en couleur, ou de documents en version provisoire.
- Utiliser la fonction « aperçu avant impression » pour vérifier le document.
- Réserver l'impression couleur aux documents contenant des visuels qui le nécessitent.

3.4 Poste téléphonique fixe :

L'utilisation du téléphone fixe est réservée à des fins professionnelles.

En cas d'absence, l'utilisateur doit :

- Effectuer un renvoi d'appels vers le poste d'un autre utilisateur habilité à recevoir et traiter ses appels
- Rediriger les appels vers le service d'accueil du site sur lequel il est basé.

3.5 Téléphone mobile :

Un téléphone mobile peut être mis à la disposition des utilisateurs pour un usage exclusivement professionnel.

Le salarié devra fournir une facture pour justifier qu'il bénéficie d'une ligne personnelle.

A ce titre, l'utilisateur est tenu :

- D'en prendre soin et de se conformer aux prescriptions d'usage,
- D'informer immédiatement la direction en cas de dysfonctionnement, de blocage, de perte ou de vol de l'équipement.

Il est rappelé que selon le code de la route, l'usage d'un téléphone par le conducteur d'un véhicule en circulation est interdit.

Si le téléphone mobile autorise une connexion à internet et à la messagerie, les utilisateurs devront respecter les obligations et interdictions visées au présent points « internet » et messagerie » ci-dessous.

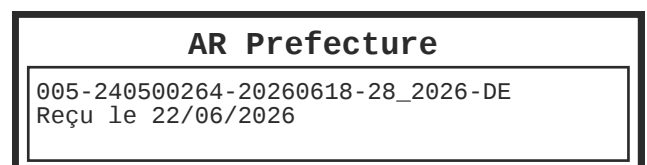
A noter que toute utilisation abusive et non professionnelles pourrait faire l'objet de sanction.

3.6 Logiciels :

- L'utilisateur ne peut installer un logiciel (payant ou gratuit), que ce soit par copie, téléchargement ou tout autre moyen, qu'après accord de la direction et supervision par le prestataire informatique.
- L'installation est également soumise à une validation préalable de la demande formalisée par le responsable hiérarchique de l'utilisateur.
- Aucune copie de logiciel non libre (non appartenant au domaine public) n'est autorisée, sauf pour les copies de sauvegarde.
- L'utilisation ou la diffusion de logiciels piratés constitue un délit, et leur diffusion peut être considérée comme du recel.

3.7 Signature électronique et certificat :

Certains utilisateurs, dans le cadre de leurs fonctions, sont amenés à utiliser des certificats de signature électronique pour signer des documents et/ou s'authentifier afin d'accéder à des services sécurisés.



Caractéristiques des certificats :

Nominatifs et non cessibles

Composés de trois éléments indissociables :

1. Informations sur l'identité du titulaire : organisation, fonction, période de validité, et autorité de certification émettrice
2. Clé privée
3. Clé publique

Obligations de l'utilisateur :

- Garder strictement confidentiel le code associé à la clé privée lors de la signature.
- Toute demande de nouveau certificat ou de renouvellement doit être validée par le responsable hiérarchique et transmise à la direction.

Durée et révocation :

- La durée de vie des certificats est limitée, généralement de 1 à 3 ans.
- Les certificats seront révoqués dans les cas suivants :
 - L'utilisateur quitte la collectivité ou n'a plus l'habilitation pour l'utiliser
 - Perte du certificat
 - Compromission de la clé privée

3.8 Pack office 365 :

Les utilisateurs disposent d'un pack Office 365.

L'accès se fait via un identifiant et un mot de passe personnel.

Utilisation de la messagerie

La messagerie électronique nominative est destinée uniquement à un usage professionnel. Cette dernière peut être installée sur un autre périphérique (tablette ou téléphone). L'utilisateur sera garant de la sécurité de son périphérique

Règles générales d'utilisation :

- Vérifier la liste des destinataires avant l'envoi et utiliser la fonction Cci pour protéger les adresses.
- En cas d'absence, activer un message automatique précisant la date de retour et, le cas échéant, la personne ou le service à contacter.
- Pour les transmissions de fichiers internes, il est recommandé de partager le chemin d'accès sur le réseau plutôt que d'envoyer le fichier en pièce jointe.

Contrôles et usages interdits

La collectivité se réserve le droit d'effectuer des contrôles en cas de mauvaise utilisation grave notamment :

- Envoyer ou recevoir des informations dont le contenu ou la forme peut nuire à la collectivité.
- Diffuser des informations confidentielles sur l'organisation, le personnel ou les élus.
- Envoyer des messages engageant la responsabilité contractuelle de la collectivité.

Les mêmes règles s'appliquent aux boîtes aux lettres professionnelles génériques.

Comportement et actes illicites

- Les messages à caractère discriminatoire (sexe, état de santé, handicap, appartenance ethnique, orientation sexuelle) sont strictement interdits.
- Les messages exprimant des opinions philosophiques ou religieuses sont également proscrits.



Responsabilité vis-à-vis des messages illicites

- Un agent ne peut être tenu responsable s'il reçoit, à son insu, des messages à caractère discriminatoire ou illicite.
- Il est néanmoins imposé à l'utilisateur de ne pas relayer ces messages.
- L'utilisateur ne doit pas solliciter l'envoi de tels messages, ni participer à des groupes de discussion ou consulter des sites dont le contenu est proscriit et qui pourraient enregistrer ses coordonnées.

Utilisation personnelle de la messagerie

- Tout message reçu ou envoyé depuis le poste de travail est, par principe, à usage professionnel.
- La collectivité pratique toutefois une tolérance limitée pour une utilisation personnelle.
- L'utilisateur doit identifier clairement les messages personnels pour que leur caractère privé soit respecté.

Accès aux données par la collectivité

- Les données stockées sur un ordinateur professionnel ou sur la messagerie sont par défaut considérées comme professionnelles, et la collectivité se réserve le droit d'y accéder.
- L'accès aux fichiers et dossiers identifiés comme personnels peut se faire :
 - En présence de l'utilisateur, ou après l'avoir invité à être présent.
 - En son absence, sans information préalable, en cas d'événement ou de risque particulier pour l'organisation.
- En cas de litige, seuls les tribunaux sont compétents pour apprécier le caractère particulier de l'événement ou du risque. La CNIL n'est pas compétente sur ce point.

Remarque importante : par défaut, les fichiers stockés sur l'ordinateur professionnel ont un caractère professionnel et peuvent être consultés par l'employeur.

4. MOYENS DESTINES A ASSURER LA SECURITE INFORMATIQUE :

4.1 Compte utilisateur et mot de passe

- Chaque utilisateur du réseau informatique se voit attribuer un compte, associé à un identifiant et à un mot de passe.
- L'utilisateur est responsable de l'utilisation de ce compte et ne doit pas communiquer son mot de passe à une tierce personne.
- Le mot de passe ne doit pas être noté sur un support quelconque et est inaccessibles et intransmissible par nature.

Identification et sécurité

- L'utilisateur doit s'identifier clairement.
- Usurper l'identité d'autrui ou agir de façon anonyme est strictement interdit.
- L'utilisateur doit verrouiller ou fermer sa session lorsqu'il quitte son poste (par exemple, via la combinaison Windows + L).
- Sans déconnexion, la messagerie et les répertoires personnels restent accessibles à tout utilisateur suivant.

Politique de mot de passe

- La direction applique une politique de mot de passe conforme aux préconisations de l'ANSSI (Agence nationale de la sécurité des systèmes d'information).
 - Changement régulier tous les 90 jours



- Longueur et complexité minimale
- Le mot de passe doit comporter au moins 14 caractères, incluant :
 - Au moins une lettre majuscule et une lettre minuscule
 - Au moins un chiffre et/ou un caractère spécial
- Il ne doit pas contenir le nom ou prénom de l'utilisateur ni ceux de la collectivité

4.2 Dispositifs de préventions des virus informatiques :

La direction a mis en place un système antivirus (Service Managé) qui contrôle les flux externes (Internet) et internes sur le réseau, afin d'intercepter et d'éliminer les virus informatiques.

Obligations des utilisateurs

Pour limiter les risques de diffusion de virus, il est strictement interdit :

- D'introduire des supports externes (clés USB, CD-ROM...) provenant de sources non sécurisées
- De connecter à son poste des équipements personnels (smartphones, tablettes, etc.)
- D'installer des logiciels externes qu'après accord de la direction et supervision par le prestataire informatique.

Bonnes pratiques

- Se méfier des fichiers transmis par messagerie qui semblent suspects ou provenant d'expéditeurs inconnus.
- En cas de doute, s'adresser immédiatement le référent informatique et prévenir le prestataire Informatique.
- En cas de fonctionnement inhabituel du poste informatique (lenteur du système ou du réseau, comportements anormaux), prévenir le référent informatique sans délai.

4.3 Prévention des risques liés à la messagerie électronique :

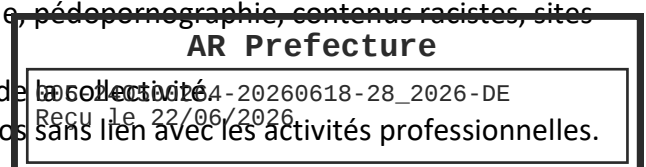
La messagerie constitue l'un des principaux vecteurs de propagation des virus et d'attaques de type phishing (techniques visant à collecter frauduleusement des informations personnelles ou confidentielles).

- Des outils de protection ont été mis en place : tout message infecté détecté par le système sera éradiqué automatiquement par réparation ou suppression.
- Cependant, il est impossible de garantir une sécurité totale, d'où la nécessité de respecter les précautions suivantes :
 - Ne pas ouvrir les messages suspects : non sollicités, objet douteux, expéditeur inconnu, liens ou pièces jointes suspectes. Signaler ces messages à la direction ou les supprimer directement.
 - Ne pas répondre à une demande d'informations confidentielles (mot de passe, code PIN, coordonnées bancaires) reçue par mail, ni compléter des formulaires en ligne.
 - En cas de doute sur l'expéditeur, vérifier son identité avant toute action pour éviter l'usurpation.
 - Informer immédiatement la direction en cas de messages non sollicités récurrents ou manifestement illicites.

4.4 Utilisation d'Internet :

Les utilisateurs disposant d'un accès à Internet pour leurs fonctions professionnelles doivent respecter les règles suivantes :

- Ne pas accéder à des sites illicites : pornographie, pédopornographie, contenus racistes, sites de jeux d'argent, etc.
- Ne pas visiter de sites pouvant nuire à l'intérêt de la collectivité.
- Ne pas télécharger des logiciels, vidéos ou photos sans lien avec les activités professionnelles.



4.5 Utilisation des réseaux sociaux :

- L'utilisation des réseaux sociaux est réservée à des fins professionnelles.
- Cette utilisation doit être appropriée et respecter le devoir de réserve.
- Il est obligatoire de distinguer l'usage professionnel de l'usage personnel, notamment par la création de profils distincts pour chaque usage

4.6 Le télétravail :

Le télétravail désigne une organisation du travail dans laquelle un travail, pouvant être réalisé dans les locaux de l'administration, est exécuté par un agent hors des locaux, de façon régulière et volontaire, en utilisant les technologies de l'information et de la communication.

Droits et obligations :

- Le télétravailleur bénéficie des mêmes droits et est soumis aux mêmes obligations que les agents travaillant sur site, tels que décrits dans la présente charte.

Bonnes pratiques spécifiques au télétravail :

- Vérifier le paramétrage de votre box Internet : changer le mot de passe administrateur s'il est faible.
- Utilisation obligatoire du VPN pour accéder aux dossiers de la collectivité.
- Interdiction de stocker des fichiers sur des clés USB ou disques durs externes.
- Les mots de passe ne doivent pas être stockés sur un support non sécurisé.
- En télétravail, respecter les mêmes règles de comportement que celles applicables au bureau.

5. DROITS ET DEVOIRS DES UTILISATEURS :

5.1 Principe généraux :

Les utilisateurs doivent :

- Appliquer les recommandations de sécurité inscrites dans la présente charte.
- Respecter les règles de bon usage afin d'éviter toute opération susceptible de nuire à la collectivité.

À ce titre, ces derniers :

- Disposent d'un droit d'accès strictement personnel et incessible.
- Contribuent à la sécurité informatique, en signalant tout dysfonctionnement ou anomalie des ressources utilisées.
- Utilisent les logiciels dans le respect de la propriété intellectuelle et des droits d'auteur, et ne doivent pas reproduire ou diffuser des données protégées sans autorisation.
- Ne doivent pas introduire de ressources extérieures, matérielles ou logicielles, susceptibles de compromettre la sécurité du système d'information et de communication.
- Effectuent des sauvegardes régulières pour les fichiers autres que ceux déjà sauvegardés automatiquement sur le réseau.

L'utilisation des moyens informatiques et télécom doit être strictement professionnelle, dans le cadre des missions de service public de la collectivité, et réalisée de manière loyale et responsable.

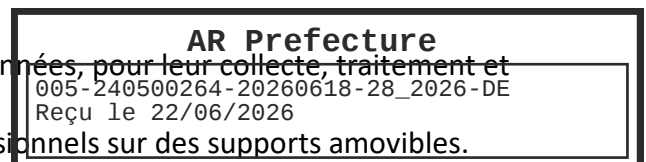
5.2 Respect de la confidentialité des données :

Répartition des droits d'accès :

Les utilisateurs, dans le cadre de leurs missions et compétences, sont amenés à gérer des fichiers dont la confidentialité doit être garantie.

Ils doivent veiller à :

- Respecter l'intégrité et la confidentialité des données, pour leur collecte, traitement et communication interne.
- Ne pas copier ni sauvegarder les fichiers professionnels sur des supports amovibles.



- Ne pas collecter de données dont le contenu contreviendrait aux lois et règlements en vigueur. Les utilisateurs s'engagent à :
- Ne pas prendre connaissance d'informations appartenant à autrui sans autorisation.
- Ne pas communiquer à un tiers des informations non publiques auxquelles ils ont accès, mais dont ils ne sont pas propriétaires.

Informations spécifiques sur le NAS : Les données enregistrées sur le NAS sont partagées avec d'autres utilisateurs, notamment les agents du service. L'enregistrement de données à caractère personnel est strictement interdit.

Les règles de secret professionnel, déontologie, obligation de réserve et devoir de discrétion s'imposent concernant les informations présentes sur le réseau et les messages électroniques professionnels

6. LE DROIT A LA DÉCONNEXION :

Le droit à la déconnexion s'entend comme le droit pour tout agent public de ne pas être connecté à un outil numérique professionnel en dehors de son temps de travail.

Ce droit, qui s'inscrit dans une démarche d'amélioration des conditions de travail et d'une meilleure conciliation entre la vie professionnelle et la vie personnel, a pour objectif le respect des temps de repos et de congé.

Ainsi, ce droit permet aux agents publics de ne pas répondre aux sollicitations professionnelles en dehors des horaires de travail sans risque d'être sanctionnés.

Les règles suivantes peuvent être adoptées :

- Respecter les périodes de repos, congés et disponibilité de l'ensemble des agents, périodes pendant lesquelles ils ne sont pas tenus de consulter leurs messages et de répondre aux sollicitations (à l'exception des agents en astreinte).
- En tout état de cause, les élus doivent s'abstenir de contacter leurs agents en dehors de leurs horaires de travail habituels, ainsi que pendant leurs congés ou en cas d'arrêt maladie, sauf nécessité de service ou urgence caractérisée.
- Dans tous les cas, l'usage de la messagerie électronique, du téléphone professionnel ou de tout autre outil numérique en dehors des horaires de travail doit être justifié par la gravité, l'urgence et/ou l'importance du sujet en cause.

AR Prefecture

005-240500264-20260618-28_2026-DE
Reçu le 22/06/2026

RÉCÉPISSÉ CHARTE INFORMATIQUE

Je soussigné,

Nom :

Prénom :

Service :

Fonction :

Utilisateur des moyens informatiques et réseaux du SIVOM de La Grave Villar d'Arène, de la Grave et de Villar d'Arène, déclare avoir pris connaissance de la présente charte et m'engage à la respecter.

Fait à

Le

Signature

Fait en deux exemplaires :

-un pour l'intéressé (agent – élu)

-un pour la collectivité

AR Prefecture

005-240500264-20260618-28_2026-DE
Reçu le 22/06/2026