Envoyé en préfecture le 25/03/2026
Reçu en préfecture le 25/03/2026
Publié le 26/03/26
ID : 013-211300447-20260323-DEL_2026_45-DE

ville de Grans

LOI DU 5 AVRIL 1884 - ARTICLE 56

# DELIBERATION DU CONSEIL MUNICIPAL

## Séance du 23 mars 2026

L'an deux mille vingt-six et le vingt-trois mars à vingt heures, le Conseil Municipal de cette Commune, régulièrement convoqué, s'est réuni au nombre prescrit par la Loi, en Salle d'Honneur Germaine Richier de la Mairie, sous la présidence de **Monsieur Philippe LEANDRI, Maire.**

**Présents** : R. ANSILLON - V. APPOLONIE - F. ARNAUD - D. AUBERT- N. BARDIN - F. BERTORELLO – D. BUSELLI - E. CADET - R. CARTA - A. BIERREN - J. GIRARD - M. GRASSI - C. HUGUES - J-C. LAURENS - T. MARTIN - D. MIACHON - V. OLIVE - I. TEISSIER - N. REVERTER - C. RUIZ - R. SAURIN--DEVASSY - V. TIQUET - V. TRICON - G. VALVASON-SERODINE - L. VIARDOT-AMOURIC - P. VIDAL

**Procurations** : M. PERONNET à C. HUGUES – G. RAYNAUD-BREMOND à G. VALVASON-SERODINE

**Date de la convocation** : Mardi 17 mars 2026

**Secrétaire de Séance** : Eric CADET

République Française
---
**MAIRIE DE GRANS**
---
(Bouches-du-Rhône)
---
Arrondissement d'Istres

| NOMBRE DE MEMBRES | | |
|---|---|---|
| Afférents au Conseil Municipal | En Exercice | Qui ont pris part à la délibération |
| 29 | 29 | 29 |

**N° 2026/45**

**Adoption de la charte informatique**

Depuis ces dernières années, les collectivités sont confrontées à un risque de cyber attaques de plus en plus marquées. Ces attaques peuvent entraîner des conséquences préjudiciables importantes pour les collectivités : interruption des services administratifs, inaccessibilité des documents financiers ou administratifs, fuite de données à caractère personnel, indisponibilité des infrastructures, ...

Pour faire face à ces risques et dans le cadre de ses missions de sécurisation du système d'information et de protection des données, la commune s'est dotée d'une politique de sécurité des systèmes d'information.

Pour une efficacité optimale, la sécurité des règles d'utilisation repose aussi sur la mobilisation de tous : chaque agent doit en effet contribuer à la sécurité informatique en observant des règles d'utilisation des outils informatiques et une vigilance constante.

Vu le Code Général des Collectivités Territoriales,

Vu la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés,

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

Vu la loi n°83-634 du 13 juillet 1983 modifiée portant droit et obligations des fonctionnaires,

Vu la loi n°84-53 du 26 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique territoriale, imposant notamment les obligations de réserve, de discrétion et de secret professionnel aux agents publics,

Vu le décret n°2010-112 du 2 février 2010 modifié pris pour l'application des articles 9, 10 et 12 de 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,

Vu le règlement général sur la protection des données (RGPD) du 25 mai 2018 fixant les règles à respecter en matière de protection des données personnelles,

Considérant que la commune fait face à des risques de sécurité informatique croissants, il est nécessaire de mettre en place différentes mesures destinées à sécuriser son système d'information et à protéger ses données,

Considérant la nécessité de sécuriser le système informatique de la Commune, une charte informatique a été rédigée, définissant les modalités d'utilisation des outils informatiques et de télécommunications mis à disposition des agents de la ville.

Considérant la nécessité d'en assurer l'opposabilité aux utilisateurs et renforcer son efficacité, il convient d'approuver la charte informatique,

Envoyé en préfecture le 25/03/2026
Reçu en préfecture le 25/03/2026
Publié le 26/03/26
ID : 013-211300447-20260323-DEL_2026_45-DE

ville de Grans

LOI DU 5 AVRIL 1884 - ARTICLE 56

# DELIBERATION DU CONSEIL MUNICIPAL

## Séance du 23 mars 2026

L'an deux mille vingt-six et le vingt-trois mars à vingt heures, le Conseil Municipal de cette Commune, régulièrement convoqué, s'est réuni au nombre prescrit par la Loi, en Salle d'Honneur Germaine Richier de la Mairie, sous la présidence de **Monsieur Philippe LEANDRI, Maire.**

**Présents** : R. ANSILLON - V. APPOLONIE - F. ARNAUD - D. AUBERT- N. BARDIN - F. BERTORELLO – D. BUSELLI - E. CADET - R. CARTA - A. BIERREN - J. GIRARD - M. GRASSI - C. HUGUES - J-C. LAURENS - T. MARTIN - D. MIACHON - V. OLIVE - I. TEISSIER - N. REVERTER - C. RUIZ - R. SAURIN--DEVASSY - V. TIQUET - V. TRICON - G. VALVASON-SERODINE - L. VIARDOT-AMOURIC - P. VIDAL

**Procurations** : M. PERONNET à C. HUGUES – G. RAYNAUD-BREMOND à G. VALVASON-SERODINE

**Date de la convocation** : Mardi 17 mars 2026

**Secrétaire de Séance** : Eric CADET

République Française
---
**MAIRIE DE GRANS**
---
(Bouches-du-Rhône)
---
Arrondissement d'Istres

| NOMBRE DE MEMBRES | | |
|---|---|---|
| Afférents au Conseil Municipal | En Exercice | Qui ont pris part à la délibération |
| 29 | 29 | 29 |

**N° 2026/45**

**Adoption de la charte informatique**

Le Conseil Municipal, à l'unanimité, l'exposé de Monsieur Le Maire entendu,

- Adopte la charte informatique.
- Autorise Monsieur le Maire ou son représentant dûment habilité à signer la présente délibération ainsi que toutes pièces utiles afin de mener à bien cette affaire.

Conformément à l'article R421-1 du Code de Justice Administrative, le présent acte pourra faire l'objet d'un recours contentieux devant le Tribunal Administratif de MARSEILLE, sis 31 rue Jean François Leca – 13002 MARSEILLE (tél. : 04.91.13.48.13 / Courriel : greffe.ta-marseille@juradm.fr) dans un délai de deux (02) mois à compter de sa publication. Un recours administratif est également possible auprès de l'autorité du présent acte dans le délai de deux (02) mois à compter de sa publication.
Cette démarche prolonge le délai de recours contentieux qui doit alors être introduit dans les deux (02) mois suivant la notification de la décision de rejet express du recours administratif ou à compter de la date d'expiration du délai de réponse de deux mois dont disposait l'autorité signataire, en cas de rejet implicite dudit recours. Toute saisine du Tribunal Administratif de MARSEILLE peut s'opérer par voie postale, soit par voie électronique à partir de l'application internet « Télérecours citoyens » accessible par le site de téléprocédures : http:// www.telerecours.fr/

Fait en séance, les jour, mois et an susdits,
ont signé au registre les membres présents,
Le Maire, Philippe LEANDRI

Le secrétaire de séance,
Eric CADET

MAIRIE DE GRANS
Bouches-du-Rhône

Envoyé en préfecture le 25/03/2026
Reçu en préfecture le 25/03/2026
Publié le 26/03/26
ID : 013-211300447-20260323-DEL_2026_45-DE

# CHARTE D'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (T.I.C.)

Envoyé en préfecture le 25/03/2026
Reçu en préfecture le 25/03/2026
Publié le 26/03/26
ID : 013-211300447-20260323-DEL_2026_45-DE

# Sommaire

1. PREAMBULE ..... 3
**1.1 Le contexte et les enjeux ..... 3**
**1.2 L'objectif ..... 3**
**1.3 Le champ d'application ..... 3**
2. LES REGLES GENERALES D'UTILISATION ..... 3
**2.1 Les droits et les devoirs des utilisateurs ..... 4**
2.1.1 Un accès aux ressources règlementé ..... 4
2.1.2 Une utilisation professionnelle des ressources ..... 4
**2.2 Les droits et les devoirs de la collectivité ..... 4**
**2.3 L'analyse et le contrôle ..... 5**
**2.4 Les sanctions ..... 5**
**2.5 Les évolutions ..... 5**
3. LES POSTES INFORMATIQUES ..... 5
4. LA MESSAGERIE ..... 6
5. L'INTERNET ..... 7
6. LE TELEPHONE ..... 8
7. LES BASES LEGALES ..... 8
**7.1 Les textes législatifs ..... 8**
**7.2 Le droit disciplinaire ..... 9**
**7.3 Le code pénal ..... 9**
**7.4 La règlementation européenne ..... 10**
8. GLOSSAIRE ..... 10

# 1. PREAMBULE

## 1.1 LE CONTEXTE ET LES ENJEUX

Les différents outils technologiques utilisés offrent au personnel une grande ouverture vers l'extérieur. Cette ouverture peut apporter des améliorations de performances importantes si l'utilisation de ces outils technologiques est effectuée à bon escient et selon certaines règles.
A l'inverse, une mauvaise utilisation de ces outils peut entraîner des conséquences extrêmement graves. En effet, ils augmentent les risques d'atteinte à la confidentialité, de mise en jeu de la responsabilité, d'atteinte à l'intégrité et à la sécurité des fichiers de données personnelles (virus, intrusions sur le réseau interne, vols de données). De plus, mal utilisés, les outils informatiques peuvent aussi être une source de perte de productivité et de coûts additionnels.
L'application des nouvelles technologies informatiques et de communication permettent de préserver le système d'information, le bon fonctionnement des services et les droits et libertés de chacun.

## 1.2 L'OBJECTIF

La présente charte informatique est un code de déontologie formalisant les règles légales et de sécurité relatives à l'utilisation de tout système d'information et de communication au sein de la collectivité : applications métiers, bureautique, messagerie, micro -ordinateurs fixes et portables, périphériques, téléphones fixes et portables, Internet, Extranet, Intranet (liste non exhaustive).
Tout manquement, selon sa gravité, est susceptible d'entraîner pour l'utilisateur des sanctions disciplinaires, et ce sans exclusion d'éventuelles actions pénales ou civiles à son encontre.
L'utilisateur pourra, en outre, voir ses droits d'accès aux ressources et système d'information et de communication suspendus ou supprimés, partiellement ou totalement.

## 1.3 LE CHAMP D'APPLICATION

La présente charte s'applique à l'ensemble du personnel tous statuts confondus, ainsi qu'au personnel temporaire et aux élus. Elle s'applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques de la collectivité. Tout contrat avec un prestataire extérieur devra faire référence et comporter comme annexe la présente charte.
Dès l'entrée en vigueur de la présente charte, chaque agent de la collectivité s'en verra remettre un exemplaire, il devra en prendre connaissance et devra s'engager à la respecter.

# 2. LES REGLES GENERALES D'UTILISATION

Les utilisateurs sont supposés adopter un comportement responsable s'interdisant par exemple toute tentative d'accès à des données ou à des sites qui leurs seraient interdits.
Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie et s'engage à ne pas effectuer d'opérations qui pourraient entraîner des conséquences néfastes sur le fonctionnement du réseau. Il doit en permanence garder à l'esprit que c'est sous le nom de la collectivité qu'il se présente sur Internet et doit se porter garant de l'image de l'institution.
Au même titre que pour le courrier, le téléphone ou la télécopie, chacun est responsable des messages envoyés ou reçus, et doit utiliser la messagerie dans le respect de la hiérarchie, des missions et fonctions qui lui sont dévolues et des règles élémentaires de courtoisie et de bienséance.

Envoyé en préfecture le 25/03/2026
Reçu en préfecture le 25/03/2026
Publié le 26/03/26
ID : 013-211300447-20260323-DEL_2026_45-DE

## 2.1 LES DROITS ET LES DEVOIRS DES UTILISATEURS

### 2.1.1 UN ACCÈS AUX RESSOURCES RÈGLEMENTÉ

Toute personne (agent et élu) travaillant dans la collectivité dispose d'un droit d'accès au système d'information. Ce droit d'accès est :

- Strictement personnel,
- Incessible

### 2.1.2 UNE UTILISATION PROFESSIONNELLE DES RESSOURCES

Les ressources informatiques mises à disposition constituent un outil de travail nécessaire.
Chaque utilisateur doit adopter une attitude responsable et respecter les règles définies sur l'utilisation des ressources et notamment :

- Respecter l'intégrité et la confidentialité des données. Cette règle s'applique tant pour le traitement des informations que pour leur communication interne et externe.
- Ne pas perturber la disponibilité du système d'information.
- Ne pas stocker ou transmettre d'informations portant atteinte à la dignité humaine.
- Ne pas marquer les données exploitées d'annotations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et images de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée (loi " informatique et liberté " du 06/01/1978). Une déclaration à la CNIL est obligatoire pour toute création de fichiers contenant des informations nominatives.
- Respecter le droit de propriété intellectuelle : non reproduction et/ou non-diffusion de données soumises à un droit de copie non-détenu, interdiction de copie de logiciel sans licence d'utilisation.
- Ne pas introduire de "ressources extérieures" matérielles ou logicielles qui pourraient porter atteinte à la sécurité du système d'information.
- Respecter les contraintes liées à la maintenance du système d'information.
- Ne pas masquer son identité ou usurper celle d'un autre.

L'usage de ces outils de communication ne modifie en rien les obligations de validation et d'information vis-à-vis de la hiérarchie.

La continuité du service étant une priorité, l'utilisateur s'interdit, cependant, d'appliquer des mesures de sécurité non validées par la Direction Générale des Services et qui auraient pour conséquence de rendre inaccessibles des informations intéressant le bon fonctionnement de la collectivité (chiffrement ou protection d'un fichier à l'aide d'un mot de passe non communiqué à son supérieur hiérarchique, par exemple).
Les droits d'accès peuvent être modifiés ou retirés à tout moment, selon les besoins du service, et prennent fin lors de la cessation de l'activité professionnelle.

## 2.2 LES DROITS ET LES DEVOIRS DE LA COLLECTIVITÉ

La collectivité doit veiller à la disponibilité et à l'intégrité du système d'information.
En ce sens, elle s'engage à :

- Mettre à disposition les ressources informatiques matérielles et logicielles nécessaires au bon déroulement de la mission des utilisateurs.
- Mettre en place des programmes de formations adaptés et nécessaires aux utilisateurs pour une bonne utilisation des outils.

Envoyé en préfecture le 25/03/2026
Reçu en préfecture le 25/03/2026
Publié le 26/03/26
ID : 013-211300447-20260323-DEL_2026_45-DE

- Informer les utilisateurs des diverses contraintes d'exploitation (interruption de service, maintenance, modification de ressources...) du système d'information susceptibles d'occasionner une perturbation.
- Effectuer les mises à jour nécessaires des matériels et des logiciels composant le système d'information afin de maintenir le niveau de sécurité en vigueur dans le respect des règles d'achat et des budgets alloués.
- Respecter la confidentialité des "données utilisateurs" auxquelles il pourrait être amené à accéder pour diagnostiquer ou corriger un problème spécifique.
- Définir les règles d'usage de son système d'information et veiller à leur application.

### 2.3 L'ANALYSE ET LE CONTRÔLE

Pour des nécessités de sécurité, de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent, sous le contrôle du responsable informatique et de l'autorité territoriale, être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi relative à l'informatique, aux fichiers et aux libertés.

### 2.4 LES SANCTIONS

La loi, les textes réglementaires et la présente charte définissent les droits et obligations des personnes utilisant les ressources informatiques.

Tout utilisateur du système d'information de la collectivité n'ayant pas respecté la loi pourra être poursuivi pénalement.

En outre, tout utilisateur ne respectant pas les règles définies dans cette charte est passible de mesures qui peuvent être internes à l'établissement et/ou de sanctions disciplinaires proportionnelles à la gravité des manquements constatés par l'autorité territoriale

### 2.5 LES EVOLUTIONS

Avant son entrée en vigueur, la présente charte a été soumise à l'avis du Comité Social Territorial. Elle pourra être complétée ou modifiée par l'autorité territoriale, l'avis du Comité Social Territorial sera à nouveau demandé.

## 3. LES POSTES INFORMATIQUES

Cette présente partie a pour objectif d'établir les règles d'utilisation des postes. Un ensemble "matériels - système d'exploitation -logiciels" est mis à disposition de chaque utilisateur :

- Matériel : unité centrale, écran, clavier, souris...
- Système d'exploitation : Windows toutes versions...
- Logiciel : pack bureautique, logiciels de communication, logiciels de gestion, applications spécifiques.

Le matériel informatique est fragile, il faut en prendre soin et redoubler d'attention pour les écrans plats.

Les supports amovibles (CD ROM, clé USB, etc.) provenant de l'extérieur doivent être soumis à un contrôle antivirus préalable.

Toute installation logicielle est à la charge de la personne compétente et désignée par l'autorité territoriale.

Les téléchargements à l'initiative de l'utilisateur et sans l'autorisation du responsable informatique sont interdits.

En cas d'absence momentanée, l'utilisateur doit verrouiller son PC (Ex. : maintenir enfoncées les touches "Ctrl+Alt+Suppr'" et cliquer sur "Verrouiller l'ordinateur"). En cas d'absence, l'utilisateur doit quitter les applications et verrouiller systématiquement son PC. *Attention, cette méthode peut être différente en fonction du matériel informatique.*
A la fin de sa journée de travail, l'utilisateur doit quitter les applications, arrêter le système par arrêt logiciel, éteindre l'écran et l'imprimante.

Un premier niveau de sécurité consiste à utiliser des mots de passe sûrs non communiqués à des tiers et régulièrement modifiés (au moins deux fois par an).

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde quotidienne des informations.

L'utilisateur doit signaler tous dysfonctionnements ou anomalies au service ou référent informatique selon la procédure définie par la collectivité.

L'utilisateur doit procéder régulièrement à l'élimination des fichiers non-utilisés et à l'archivage dans le but de préserver la capacité de mémoire

## 4. LA MESSAGERIE

Cette présente partie a pour objectif d'établir les règles d'utilisation de la messagerie électronique.

L'utilisation de la messagerie est réservée à des fins professionnelles. Néanmoins il est toléré en dehors des heures de travail un usage modéré de celle-ci pour des besoins personnels et ponctuels.

L'utilisateur est tenu de la consulter au minimum une fois par jour, hormis en période d'absence. Il doit accorder la même importance aux messages électroniques qu'aux courriers postaux et se doit de les traiter.

La lecture des courriels personnels reçus durant les heures de travail est tolérée si celle-ci reste occasionnelle.

L'utilisateur veillera à ne pas ouvrir les courriels dont le sujet paraîtrait suspect.

Tout courrier électronique est réputé professionnel et est donc susceptible d'être ouvert par l'autorité territoriale ou le référent informatique. Les courriers à caractère privé et personnel doivent expressément porter la mention « personnel et confidentiel » dans leur objet. Ces derniers ne pourront alors être ouverts par l'autorité territoriale ou le référent informatique, que pour des raisons exceptionnelles de sauvegarde de la sécurité ou de préservation des risques de manquement de droit des tiers ou à la loi.

L'utilisateur s'engage à ne pas envoyer en dehors des services de la collectivité des informations professionnelles nominatives ou confidentielles, sauf si cet envoi est à caractère professionnel et autorisé par son supérieur hiérarchique.

L'utilisateur soigne la qualité des informations envoyées à l'extérieur et s'engage à ne pas diffuser d'informations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.

L'utilisateur signera tout courriel professionnel. Elle comportera obligatoirement :

- Le nom et prénom de l'expéditeur ;
- Son entité de rattachement ;

Envoyé en préfecture le 25/03/2026
Reçu en préfecture le 25/03/2026
Publié le 26/03/26
ID : 013-211300447-20260323-DEL_2026_45-DE

L'utilisateur doit vérifier la liste des destinataires et respecter les circuits de l'organisation ou la voie hiérarchique le cas échéant.

L'utilisateur doit éviter de surcharger le réseau d'informations inutiles. Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier « éléments supprimés » doit être vidé périodiquement.

En cas d'absence prévisible, l'utilisateur devra mettre en place un message automatique d'absence indiquant la date de retour prévue. Un agent du service doit pouvoir gérer les messages pendant son absence.

La signature électronique (loi n° 2000-230 du 13 mars 2000) est présumée fiable jusqu'à preuve du contraire. Son utilisation est limitée aux personnes autorisées et doit respecter la procédure définie par la collectivité.

Une équivalence juridique est établie entre le courrier électronique et le courrier sur support papier (ordonnance du 8 décembre 2005). Ils doivent, en conséquence être traités dans les mêmes délais.

## 5. L'INTERNET

Cette présente partie a pour objectif d'établir les règles d'utilisation de l'Internet.

L'utilisation d'Internet est réservée à des fins professionnelles et/ou syndicales ou associatives dans le cadre de l'exercice des décharges d'activité et autorisations spéciales d'absence.

Néanmoins, il est toléré en dehors des heures de travail un usage modéré de l'accès à Internet pour des besoins personnels à condition que la navigation n'entrave pas l'accès professionnel.

L'utilisateur s'engage lors de ses consultations Internet à ne pas se rendre sur des sites portant atteinte à la dignité humaine (pédo-pornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée,...).

Le téléchargement, en tout ou partie, de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.) est strictement interdit.
Le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet est interdit.

Tout abonnement payant à un site web ou à un service via Internet doit faire l'objet d'une autorisation préalable de l'autorité territoriale.

Pour éviter les abus, l'autorité territoriale peut procéder, à tout moment, au contrôle des connexions entrantes et sortantes et des sites les plus visités.

Toute saisie d'informations sur un site Internet professionnel nécessite l'autorisation préalable de l'autorité territoriale.

Toute procédure d'achats personnels sur Internet est formellement interdite.

L'utilisation de forums de discussion est autorisée pour un usage professionnel. Tout utilisateur participant à un forum fait figurer en bas de chacun des messages publiés la mention suivante :
« Le contenu de ce message n'engage que son auteur et en aucun cas la collectivité de GRANS ».

L'utilisation des services de messagerie instantanée, « chat », est interdite, sauf autorisation expresse de la Direction Générale des Services.

## 6. LE TELEPHONE

Cette présente partie a pour objectif d'établir les règles d'utilisation du téléphone.

L'utilisation des téléphones fixes et portables est réservée à des fins professionnelles.
Néanmoins, un usage ponctuel du téléphone pour des communications personnelles locales est toléré à condition que cela n'entrave pas l'activité professionnelle.

L'utilisation des téléphones portables personnels doit rester occasionnelle et discrète.

L'autorité territoriale peut procéder au contrôle de l'ensemble des appels émis.

En cas d'absence, l'utilisateur doit effectuer un renvoi sur le poste d'un autre agent du service ou sur l'accueil téléphonique de la Mairie.

L'agent qui quitte définitivement la collectivité doit restituer le téléphone portable professionnel.

L'utilisateur doit veiller à soigner sa présentation lors d'un appel pour faciliter son identification et/ou son service.

## 7. LES BASES LEGALES

L'utilisateur doit respecter les obligations de réserve, de discrétion et de secret professionnel conformément aux droits et obligations des agents publics tels que définis par la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires et la loi n°84-53 du 26 janvier 1984 relative à la fonction publique territoriale.

Cette présente partie a pour objectif d'informer les utilisateurs des textes législatifs et réglementaires dans le domaine de la sécurité des systèmes d'information.

### 7.1 LES TEXTES LÉGISLATIFS

- Loi du 06/01/1978 relative à l'informatique, aux fichiers et aux libertés. Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.

- Loi du 17/07/1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

- Loi du 03/07/1985 relative aux droits d'auteur et aux droits des artistes - interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle. Elle interdit à l'utilisateur d'un logiciel toute reproduction de celui-ci autre que l'établissement d'une copie de sauvegarde.

- Loi du 05/01/1988 sur la fraude informatique. Cette loi, dite de GODEFRAIN, vise à lutter contre la fraude informatique en réprimant :
  - Les accès ou maintien frauduleux dans un système d'information
  - Les atteintes accidentelles ou volontaires au fonctionnement
  - La falsification des documents informatiques et leur usage illicite
  - L'association ou l'entente en vue de commettre un de ces délits

- Loi du 10/07/1991 relative au secret des correspondances émises par voie des télécommunications.

- Loi du 13/03/2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

- Loi du 21/06/2004 pour la confiance dans l'économie numérique. Elle est destinée à favoriser le développement du commerce par Internet, en clarifiant les règles pour les consommateurs et les prestataires aussi bien techniques que commerciaux.

### 7.2 LE DROIT DISCIPLINAIRE

- Loi n°84 - 53 du 26 janvier 1984 (art. 89 et 90) et le décret n° 89 - 677 du 18 septembre 1989 relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux

- Décret n°92 - 1194 du 4 novembre 1992 (art. 6) fixant les dispositions communes applicables aux fonctionnaires stagiaires de la Fonction Publique Territoriale.

- Décret n°88 -45 du 15 février 1988 (art. 36 et 37) relatif aux agents non titulaires.

- Décret n°91-298 du 20 mars 1991 (art. 15) relatif aux agents à temps non complet.

### 7.3 LE CODE PÉNAL

- Article 323 - 1 : Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 € d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 € d'amende.

- Article 323 - 2 : Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 € d'amende.

- Article 323-3 : Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 € d'amende.

- Article 323 – 3 - 1 : Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323 - 1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

- Article 323-4 : La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323 -1 à 323 - 31 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

- Article 323 - 5 : Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :
  - L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
  - L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
  - La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
  - La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
  - L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
  - L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

- L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131 - 35.

- Article 323 - 6 : Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121 - 2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131 - 38, les peines prévues par l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

- Article 323 - 7 : La tentative des délits prévus par les articles 323 - 1 à 323 -3 -1 est punie des mêmes peines.

### 7.4 LA RÈGLEMENTATION EUROPÉENNE

La convention européenne du 28/01/1991 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel.

Elle définit les principes de base de la protection des données que les Etats parties doivent concrétiser dans leur ordre juridique interne. Elle exclut en principe les entraves aux flux transfrontières de données entre les Etats parties. Elle règle la coopération entre Etats pour la mise en œuvre de la Convention, en particulier l'assistance qu'un Etat partie doit prêter aux personnes concernées ayant leur résidence à l'étranger. Enfin, elle met en place un Comité consultatif chargé en particulier de faciliter et d'améliorer son application.

La directive 95/46/CE relative à la protection des données personnelles et à la libre circulation de ces données, publiée au Journal Officiel des Communautés Européennes du 23 novembre 1995. Cette directive vise à réduire les divergences entre les législations nationales sur la protection des données afin de lever tout obstacle à la libre circulation des données à caractère personnel à l'intérieur de l'Union européenne.

La directive de la CEE du 21/12/1988 sur l'harmonisation de la protection juridique des logiciels.
Elle protège les droits d'auteur, elle interdit en particulier à l'utilisateur d'un logiciel toute reproduction autre que l'établissement d'une copie de sauvegarde.

## 8. GLOSSAIRE

- SYSTEME D'INFORMATION :

Ensemble des éléments participant à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'organisation de la collectivité.

- RESSOURCES INFORMATIQUES :
  - Le matériel
  - Les logiciels et les procédures
  - Les données et les fichiers

- INTERNET :

Interconnexion mondiale de réseaux reposant sur un protocole appelé « Internet » et dont les applications les plus utilisées sont le courriel et les consultations de sites (Web).

- INTRANET :

Utilisation des technologies liées à Internet au sein d'un réseau local. Les principaux intérêts sont de faciliter et de rendre plus conviviale l'accès aux données par l'utilisation du navigateur et de la messagerie interne.

Envoyé en préfecture le 25/03/2026
Reçu en préfecture le 25/03/2026
Publié le 26/03/26
ID : 013-211300447-20260323-DEL_2026_45-DE

- EXTRANET :

On peut dire que c'est un « Intranet » étendu à des utilisateurs extérieurs qui, n'étant pas situés sur le réseau local, seront soumis à un accès sécurisé.

- COURRIEL :

Message électronique.

- RESEAU :

Ensemble d'ordinateurs et de machines informatiques qui communiquent grâce à une technique commune de transmission.

- PERIPHERIQUES :

Matériels connectés à un poste de travail ou directement sur le réseau local (exemples : imprimante, scanners...)

Fait à Grans,
Le 25/03/2026

**Le Maire,**
**Philippe LEANDRI**
dûment habilité par délibération n° 2026 /45 du 23 mars 2026