Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

VILLE DE
Ploufragan

Département des Côtes d'Armor
Arrondissement de Saint-Brieuc

COMMUNE DE PLOUFRAGAN
DELIBERATION
DU CONSEIL MUNICIPAL DU 10 NOVEMBRE 2026

Convocation du 4 novembre 2026

L'an deux-mille-vingt-six, le dix novembre à 19h00, le conseil municipal de la commune de PLOUFRAGAN s'est réuni en session ordinaire, à l'hôtel de ville, après convocation légale, sous la présidence de M. Bruno BEUZIT, Maire.

PRESENTS : Bruno BEUZIT, Mari COURTAS, Anthony DECRETON, Maryse LAURENT, Patrick COSSON, Annie LABBE, Pascal DUBRUNFAUT, Emmanuel LE NOA, Céline PESTEL, Maxime LE CRONC, Pascale LABBE, Abdel BELARBI, Mohamed MEZILET, Christine ORAIN, Pierre-Yves BRUNEL, Marie-Ange LE FLANCHEC, Pascal FOURNET, Viviane BOULIN, Bruno THYS, Annick MOISAN, Luc STRIDE, Aude SECONDINO, Rokiatou KEITA, Eric PRONGET, Marie PASCO, Yvon LE PERDU, Catherine PEDRON, Pascal JEGO, Maryline MORFOUASSE et Estelle BREILLOT

POUVOIRS : Pascale GALLERNE donne pouvoir à Pascale LABBE
Karine BOIVIN donne pouvoir à Anthony DECRETON
Pierre SALOU donne pouvoir à Maryse LAURENT

SECRETAIRE DE SEANCE : Anthony DECRETON

Membres en exercice : 33
Présents : 30
Votants : 33

2026-11-05 - Règlements intérieurs systèmes d'information

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), et notamment ses articles 5, 24 et 32 ;

Vu le code général des collectivités territoriales, et notamment son article L.2121-29 ;

Vu le code pénal, et notamment ses articles 323-1 à 323-8 relatifs aux atteintes aux systèmes de traitement automatisé de données ;

Vu les recommandations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et de la Commission nationale de l'informatique et des libertés (CNIL) applicables aux collectivités territoriales ;

Vu l'avis du comité social territorial du 28 octobre 2025 ;

Vu les projets de règlements intérieurs de l'usage des systèmes d'information à destination des utilisateurs, d'une part, et des administrateurs et référents applicatifs, d'autre part, annexés à la présente délibération ;

Considérant que le système d'information de la ville est indispensable à la continuité du service public et qu'il traite des données à caractère personnel dont la commune, responsable de traitement, doit garantir la sécurité et la confidentialité ;

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

Considérant l'augmentation des cyberattaques visant les collectivités territoriales et la nécessité de définir les droits et obligations des utilisateurs et des administrateurs de ce système ;

Considérant que les agents doivent être informés au préalable des règles d'usage et des dispositifs de contrôle mis en œuvre sur le système d'information ;

Après en avoir délibéré, le Conseil municipal, par vote à main levée, à l'unanimité,

- ADOPTE le règlement intérieur de l'usage des systèmes d'information à destination des utilisateurs, annexé à la présente délibération ;

- ADOPTE le règlement intérieur de l'usage des systèmes d'information à destination des administrateurs et référents applicatifs, annexé à la présente délibération ;

- DIT que ces deux règlements sont applicables à l'ensemble des utilisateurs et des administrateurs des systèmes d'information de la ville de Ploufragan, quel que soit leur statut, à compter de leur publication ;

- DIT que la prise en main des habilitations et comptes d'accès au système d'information est subordonnée à l'acceptation des règlements précités ;

- AUTORISE Monsieur le Maire ou son représentant à prendre toutes mesures nécessaires à la diffusion, à la sensibilisation et à l'application de ces règlements, et à les actualiser pour les mettre en conformité avec l'évolution de la réglementation et de la menace.

A Ploufragan, le 17 novembre 2026

Le Maire
Bruno BEUZIT

VILLE de PLOUFRAGAN (Côtes d'Armor)

Le secrétaire de séance
Anthony DECRETON

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

Direction Mutualisée des Systèmes d'Information
assistanceinfo@sbaa.fr - 02 96 63 25 40

POLITIQUE - Règlement intérieur de l'usage des systèmes d'information à destination des utilisateurs

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

Table des matières

Glossaire
Objet et champ d'application du Règlement
Utilisation des matériels et des logiciels mis à disposition
- Postes de travail
- Postes de travail partagés
- Fermeture des sessions et extinction des postes
- Equipements mobiles
- Réseau local et espace de stockage
- Appareil personnel
- Usage à l'étranger
- Stockage amovible
  - Usage professionnel
  - Usage personnel
- Imprimantes et copieurs
- Téléphonie
- Applications WEB et Logiciels
- Badges électroniques
  - Badges personnels
  - Badges liés aux équipements
- Signature électronique et certificat
- Messagerie électronique

Moyens destinés à assurer la sécurité informatique
- Compte « utilisateur » et mot de passe
- Dispositifs de prévention des virus informatiques
- Prévention des risques liés à la messagerie électronique / Règles relatives à la sécurité de la messagerie
  - Règles relatives à la sécurité des services de messagerie
  - Règles relatives à la protection contre l'hameçonnage et la fraude
- Utilisation d'Internet
- Accès aux salles serveurs et baies techniques
- Règles relatives à la protection physique
  - Prendre soin de son matériel et ne pas l'exposer au vol
  - Principe du bureau propre

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

Droits et devoirs des utilisateurs
Droit à la déconnexion
Tolérance de l'utilisation à des fins privées
En cas d'absence d'un utilisateur
Accès aux données
Information en cas d'absence
Désactivation des comptes et restitution du matériel
En cas de départ d'un utilisateur
En cas de perte ou vol
Le droit syndical
Le droit associatif
Obligation en matière de protection des données
Règles d'accès et de stockage des données professionnelles
Protection des données
Responsabilité des utilisateurs
Droits des utilisateurs
Utilisation des solutions d'intelligence artificielle générative
Utilisation des médias sociaux
Les précautions à prendre lors de l'utilisation des réseaux sociaux
Propriété intellectuelle
Règles de déontologie et d'éthique
Engagement de respect du Règlement et sanctions
Contrôle de ressources
Numérique responsable
Principaux textes de référence

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

1.Glossaire

« **Administrateur** » : Un Administrateur est défini comme toute personne, quel que soit son statut ou sa localisation qui a pour mission d'assurer le maintien en condition opérationnelle ou le paramétrage des composants des Systèmes d'Information de Saint-Brieuc Armor Agglomération, de la ville de Saint-Brieuc, de la ville de Ploufragan, du CIAS et de leurs satellites placés sous sa responsabilité.

« **Besoin d'en connaître** » : Principe selon lequel l'accès à une information, un document ou une ressource est limité aux seules personnes qui en ont **besoin dans le cadre de leurs fonctions ou missions**. Ce concept vise à **protéger les informations sensibles** en évitant qu'elles soient diffusées inutilement, même à des personnes pourtant habilitées à traiter d'autres informations du même niveau de confidentialité.

« **Confidentialité** » : L'information est dite confidentielle si l'utilisateur juge que sa connaissance par une entité tierce peut porter préjudice à sa personne, à son activité, ou à l'activité globale.

Les données d'authentification au Système d'Information (mots de passe, identifiants, etc.) sont confidentielles.

« **DMSI** » **:** Direction Mutualisée des Systèmes d'Information.

« **Données** » : Désigne les fichiers, bases de données, images, sons, textes, vidéos, flux ainsi que les informations sous format oral et écrit, informatisé ou non.

« **Données à caractère personnel** » **:** Toute information se rapportant à une personne physique identifiée ou identifiable (directement ou indirectement) : nom, prénom, numéro de téléphone, numéro d'identification, données de localisation, identifiant en ligne, photographies, etc.

« **Délégué à la Protection des Données** » **(DPD/DPO) :** Personne chargée de la protection des données personnelles au sein d'une organisation.

« **Espaces réseaux** » : Espaces de stockage partagés, accessibles via le réseau local pour permettre aux utilisateurs d'enregistrer, d'échanger et de collaborer sur des fichiers. Ils apparaissent sous forme de "disques réseau" dans l'explorateur de fichiers des ordinateurs.

« **Hameçonnage/Phishing** » **:** L'hameçonnage ou phishing en anglais est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe, etc.) et/ou bancaires en se faisant passer pour un tiers de confiance.

« **Messagerie instantanée** » **:** Service de communication permettant à plusieurs utilisateurs d'échanger des messages écrits en temps réel. Elle facilite les échanges rapides et instantanés, souvent complétés par le partage de fichiers, des appels audio ou vidéo.

« **Responsable de la Sécurité des Systèmes d'Information** » **(RSSI) :** Personne chargée du pilotage de la sécurité des Systèmes d'Information.

« **Système d'Information** » **(SI)** : Ensemble organisé de ressources (matériels, logiciels, données et procédures) qui permet de traiter, stocker, présenter, détruire et diffuser de l'information, quelle que soit sa forme (électronique, imprimée, manuscrite, vocale, etc.).

« **Utilisateur** » **:** Toute personne autorisée à accéder, stocker, utiliser ou traiter des ressources d'un Système d'Information de la Collectivité quel que soit son statut (notamment agent de droit public ou privé, élu, personnel intérimaire, stagiaire, prestataire), ou sa localisation (au sein ou hors des locaux).

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

« **Vie privée résiduelle** » : désigne la **tolérance accordée à un usage personnel limité et occasionnel des outils professionnels**, nécessaires pour gérer certains besoins personnels, sans compromettre la sécurité, la confidentialité ou l'efficacité du travail.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

2.Objet et champ d'application du Règlement

Les utilisateurs concernés

Ce règlement s'applique à l'ensemble des utilisateurs des Systèmes d'information de la collectivité, quel que soit son statut, qu'ils soient agents de droit public ou privé, personnels intérimaires, élus, stagiaires, prestataires ou toute personne ayant accès aux Systèmes d'Information (SI) de la collectivité (au sein ou en dehors des locaux).

Ce règlement présente les principes généraux et fondamentaux qui devront être appliqués par les utilisateurs lors de l'utilisation des ressources informatiques. Il a pour but de sensibiliser chacun aux enjeux de la sécurité informatique, de prévenir les risques liés à l'utilisation des technologies de l'information, de promouvoir un usage conforme aux exigences légales et réglementaires en vigueur, ainsi que d'encourager une démarche de numérique responsable.

Les systèmes d'information et de communication

Les systèmes d'information et de communication englobent les équipements informatiques, électroniques et téléphoniques de la collectivité, interconnectés ou non entre eux. Il s'agit notamment :

- des équipements informatiques : ordinateurs fixes ou portables, imprimantes multifonctions, terminaux mobiles et appareils assimilables (smartphones, tablettes numériques, etc.) ;
- de l'accès aux réseaux informatiques (sur place ou à distance) ;
- des applications ainsi que des services de communications (logiciels métiers, messagerie électronique, messagerie instantanée, solutions de transferts de fichiers, solutions collaboratives, etc.) ;
- des supports d'information amovibles (clés USB, disques durs externes, etc.).

Chaque utilisateur doit adopter un comportement en accord avec les principes de base de sécurité. Dans une logique de vigilance partagée il doit alerter ses collègues ou subordonnés en cas d'écarts aux règles de sécurité.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

3.Utilisation des matériels et des logiciels mis à disposition

L'utilisation des matériels et des logiciels mis à disposition par la collectivité doit se faire dans le respect des règles de sécurité et d'éthique, afin de garantir leur bon fonctionnement et la protection des données. Chaque utilisateur est responsable de l'usage qu'il en fait et doit veiller à les utiliser de manière appropriée et conforme aux politiques internes. Ces règles sont précisées dans les chapitres suivants.

> **Mémo**
>
> Tout utilisateur, quel que soit son poste ou son niveau de responsabilité, qui ne se sent pas à l'aise avec les outils numériques, est légitimement en droit de solliciter la DMSI ou le service des ressources humaines afin de bénéficier de formations adaptées.

3.1.Postes de travail

La collectivité met à disposition des utilisateurs des postes de travail fixes ou portables destinés à l'accomplissement des missions professionnelles. Ces postes de travail sont paramétrés et administrés à cet effet. Dans certaines situations particulières, des dérogations à ce principe peuvent être admises à condition que l'utilisateur contacte la DMSI pour une étude préalable. Cette étude consistera en une appréciation :

- des coûts induits par les besoins en matière de sécurité pour la connexion du nouvel équipement ;
- de la capacité d'intégration de l'équipement proposé dans l'environnement technique maintenu par la DMSI.

Les utilisateurs ne sont pas autorisés à apporter des modifications à la configuration matérielle et/ou logicielle de leur poste de travail ou de leur environnement de travail, ni à installer des logiciels sans obtenir au préalable une autorisation formelle de la DMSI.

3.2.Postes de travail partagés

Les postes partagés, utilisés par plusieurs personnes au sein de la collectivité, doivent faire l'objet d'une gestion rigoureuse afin de garantir la sécurité et la confidentialité des informations. Chaque utilisateur d'un poste partagé est responsable et doit :

- ne pas utiliser les fonctions d'enregistrement de mots de passe proposées par les navigateurs internet ;
- veiller à supprimer tous les fichiers personnels ou professionnels stockés en local (téléchargement) avant de fermer sa session. A ce titre, l'utilisateur doit privilégier l'enregistrement de ses documents dans les espaces réseau fournis par la DMSI ;
- veiller à se déconnecter de sa session de travail en fin de session (voir article « Fermeture des sessions et extinction des postes »).

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

3.3.Fermeture des sessions et extinction des postes

Vos postes de travail ainsi que certaines applications logicielles sont protégés par le même mot de passe utilisateur. Ainsi, chaque utilisateur doit verrouiller sa session de travail Windows dès qu'il s'absente, quelle que soit la durée de son absence (la combinaison  + L permet de le faire facilement et rapidement). Éteignez votre poste en fin de journée ou lors des pauses longues sans utilisation.

> **Conseil**
>
> L'utilisateur d'un poste partagé veille à éteindre le poste s'il est le dernier à l'utiliser dans la journée.

3.4.Equipements mobiles

Ces équipements (PC portable, tablettes, smartphones) sont mis à disposition pour un usage professionnel et ne doivent en aucun cas être utilisés par des personnes ne faisant pas partie de la collectivité.

Lorsque ces matériels sont utilisés à l'extérieur, notamment dans le cadre de réunions ou d'interventions hors des locaux de la collectivité, les utilisateurs en assurent la garde et la responsabilité. Les utilisateurs adoptent dans cette hypothèse un niveau de surveillance et de confidentialité accru et doivent veiller à ce que des tiers non autorisés ne puissent accéder à leurs équipements ni les utiliser.

En termes de sécurité et de confidentialité, les utilisateurs sont soumis aux mêmes obligations que les utilisateurs restant sur site. Ils devront suivre toutes les prescriptions complémentaires qui leur seront signifiées.

À l'extérieur de la collectivité, la connexion à des points d'accès Wi-Fi publics qui ne sont pas de confiance (par exemple à l'hôtel, la gare ou l'aéroport, etc.) est proscrite. En déplacement, je privilégie l'accès à Internet avec mon smartphone ou un partage de connexion.

> **Mémo**
>
> Certains réseaux Wi-Fi publics peuvent être des réseaux factices, créés et contrôlés par des cybercriminels dans le but d'intercepter les données personnelles et professionnelles échangées.
> Même si l'utilisation d'un VPN améliore la sécurité, il existe un risque : une déconnexion accidentelle du VPN peut vous exposer sans protection, à votre insu.

L'utilisation de l'appareil fourni par la collectivité à des fins personnelles est tolérée dans les limites définies à l'article « Tolérance de l'utilisation à des fins privées » . La collectivité se réserve le droit de supprimer, même à distance, des applications jugées « à risque ou inapproprié » installées par l'utilisateur sur l'appareil mobile fourni par la collectivité.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

3.5.Réseau local et espace de stockage

Les collectivités mettent à disposition des utilisateurs des ressources du réseau local ou en ligne afin de stocker leurs fichiers informatiques. Ces espaces de stockage peuvent être partagés avec plusieurs agents ou plusieurs services.

Leur utilisation doit respecter les consignes suivantes :

- le partage des dossiers doit être réalisé sur le principe de la nécessité d'en connaître ;
- l'usage des espaces doit être réalisé en vue d'économiser les ressources ; des réflexions doivent être portées dans chaque service pour limiter le stockage de documents obsolètes ;
- les données déposées dans les répertoires de partage « Temporaire_1_mois », par nature accessibles à tous, doivent être supprimées dès que le partage n'est plus utile ; à défaut, l'usage d'un répertoire « Projets » peut être demandé à la DMSI ;
- l'usage du disque "Privé" (B :) est à réserver aux documents personnels utiles dans le cadre de vos missions ; le stockage de documents d'ordre personnel doit être limité (article « Tolérance de l'utilisation à des fins privées »), l'utilisateur doit notamment s'interdire le stockage de musique, de photos, de films et d'autres contenus de divertissement ;
- l'usage de médias amovibles (clé et disque USB) doit être réservé aux seuls besoins ne pouvant pas être satisfaits par une autre solution (leurs conditions d'usages sont détaillées dans l'article « Stockage amovible »).

Mémo

Mes documents déposés sur mes disques « Partage » et « Privé » sont sauvegardés .

Mes documents déposés sur le disque dur de mon PC ne sont pas sauvegardés et ne seront pas repris par la DMSI en cas de problème sur mon poste.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

3.6.Appareil personnel

L'utilisation d'un appareil personnel (ordinateur portable, smartphone, tablette, etc.) pour accéder à la messagerie de la collectivité, à l'extranet et à Planeo est autorisée, sous réserve que l'utilisateur s'engage à en assurer la sécurité afin de protéger ses données ainsi que celles de la collectivité. À ce titre, il devra notamment veiller à :

- protéger l'équipement ou la session utilisateur par un mot de passe robuste, à modifier immédiatement en cas de partage avec un tiers (y compris un membre de la famille) ;
- ne pas installer de logiciels piratés ou issus de sources non fiables ;
- maintenir à jour régulièrement l'équipement et ses applications ;
- ne pas accéder à la messagerie depuis l'étranger (hors de France) ;
- réinitialiser l'appareil aux paramètres d'usine avant toute revente ou cession ;
- ne pas enregistrer les mots de passe professionnels dans les appareils personnels.

Un usage ponctuel et exceptionnel d'un équipement personnel dans un cadre professionnel est toléré, à condition qu'aucun document de la collectivité ne soit stocké sur l'appareil. L'utilisation devra se limiter à l'accès à distance à des services en ligne de la collectivité, via un navigateur web (messagerie, application en ligne, portail d'accès distant). Il convient notamment de s'interdire de télécharger des documents sur l'équipement personnel, de les modifier localement, puis de les réintégrer manuellement dans les systèmes de la collectivité. Cette pratique présente des risques de sécurité et va à l'encontre des bonnes pratiques en matière de protection des données.

L'utilisation de matériel personnel ne peut en aucun cas être imposée à un agent, que ce soit par un supérieur hiérarchique ou un élu, y compris en situation de crise (cyberattaque, urgence opérationnelle, etc.).

Il est interdit de connecter un équipement personnel ou externe (PC personnel, objet connecté, serveur de stockage, etc.) au réseau interne de nos collectivités. Seuls les équipements munis d'une étiquette d'inventaire peuvent être raccordés à une prise réseau ou au Wi-Fi interne.

> **Mémo**
>
> Les stagiaires doivent être équipés d'un ordinateur professionnel s'ils doivent accéder au SI.

Les équipements personnels ou appartenant à des visiteurs peuvent se connecter au réseau Wi-Fi « INTERNET_PUBLIC », qui offre un accès contrôlé à Internet, conforme à la réglementation en vigueur imposant l'identification et la traçabilité des utilisateurs.

> **Limite**
>
> La DMSI n'interviendra pas sur des périphériques personnels des agents ou élus.
>
> Pour les profils les plus sensibles une intégration du smartphone dans le système de gestion centralisée des équipements mobiles de la collectivité peut être opérée afin d'appliquer les règles de sécurité et de configuration.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

3.7.Usage à l'étranger

L'utilisation des équipements informatiques de la collectivité n'est autorisée à des fins professionnelles que dans l'Espace Schengen, incluant les micro-États européens. En dehors, il convient de prendre attache avec la DMSI pour se voir fournir des équipements et solutions adaptées.

Il est donc interdit d'emporter un ordinateur portable, une tablette ou un smartphone professionnel lors de ses déplacements personnels à l'étranger.

L'accès aux applications de la collectivité depuis un équipement personnel hors de France est interdit.

> **Mémo**
>
> À titre professionnel ou personnel : Je consulte et applique les recommandations du guide « Protection des moyens numériques lors des déplacements en France et à l'étranger » afin d'adopter les bonnes pratiques de sécurité.

3.8.Stockage amovible

3.8.1.Usage professionnel

L'usage de périphériques amovibles (clé USB, disque dur USB, carte SD, etc.) est toléré sur nos Systèmes d'Information. Cependant leurs usages doivent se faire dans les conditions suivantes :

- il doit être dédié à un usage professionnel ;
- il doit être fourni par la collectivité ;
- il doit si possible être chiffré ou à défaut, les données qu'il contient régulièrement purgées ;
- il ne doit en aucun cas servir à transporter des données sensibles ou confidentielles ou relevant d'un traitement de données personnelles (RGPD) ;
- il ne doit pas être utilisé pour archiver des données ;
- il ne doit pas servir à introduire des logiciels piratés ou des virus sur nos systèmes.

En cas de mauvais usage constaté ou d'abus, un blocage des ports USB pourra être opéré par la DMSI.

La connexion d'un dispositif USB appartenant à un usager doit être réalisée exclusivement sur des postes en libre-service dédié aux usagers.

> **Mémo**
>
> De manière générale il convient de privilégier les services en ligne https://cloud.sbaa.fr, ou les disques « privé » B : et « partage » S : et la messagerie pour transférer vos données.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

3.8.2.Usage personnel

L'usage de périphériques amovibles pour un besoin personnel (clé USB, disque dur USB) est interdit.

3.9.Imprimantes et copieurs

L'usage des copieurs et des imprimantes de la collectivité est strictement professionnel.

Lors de la numérisation de documents sensibles, les utilisateurs doivent récupérer les documents sur le serveur de partage dans les plus brefs délais. De plus, les impressions sensibles ou confidentielles ne doivent pas être laissées sans surveillance à proximité du copieur et doivent être récupérées immédiatement après impression.

Les utilisateurs doivent s'abstenir de reproduire, copier, diffuser des pages web, images, photographies, textes ou toutes autres créations protégées par le droit d'auteur conformément aux dispositions du Code de la propriété intellectuelle (article « Propriété intellectuelle »).

L'utilisateur utilise de manière responsable le matériel de copie et de reprographie et les impressions couleur. En cas d'utilisation abusive, les collectivités se réservent la possibilité de vérifier les volumes d'impressions effectuées.

Les imprimantes individuelles sont réservées à des usages spécifiques devant faire l'objet d'une validation préalable. Ces usages peuvent notamment concerner :

- les postes accueillant du public, lorsque des documents doivent être imprimés sur place pour remise immédiate ;
- l'impression de documents contenant des données sensibles ou confidentielles, nécessitant un niveau de confidentialité accru.

> **Conseil**
>
> Il est préconisé :
>
> - D'éviter l'impression systématique de mails (et notamment en couleur) ou de documents en version provisoire ;
> - D'utiliser la fonction « aperçu » avant d'imprimer ;
> - D'utiliser le mode d'impression couleur, uniquement pour les documents contenant des visuels le nécessitant.

3.10.Téléphonie

L'usage du téléphone mis à disposition par la collectivité (fixe ou mobile) doit être utilisé de manière responsable et professionnelle. Les utilisateurs sont tenus de ne pas divulguer d'informations sensibles ou confidentielles par téléphone sans prendre les précautions nécessaires pour vérifier l'identité de l'interlocuteur.

L'usage du téléphone est toléré pour des communications personnelles à condition qu'il soit ponctuel, qu'il concerne des appels locaux et n'entrave pas l'activité professionnelle des utilisateurs. Les systèmes téléphoniques utilisés par la collectivité disposent d'une fonctionnalité permettant de garder la trace de tout

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

appel. Une facture détaillée listant tous les numéros appelés peut être demandée à l'opérateur en cas de besoin, notamment si la consommation de l'utilisateur est jugée excessive.

En cas d'utilisation abusive à des fins personnelles (appel vers des numéros surtaxés, envois de sms vers des services payants, appel vers ou depuis l'étranger), le remboursement des coûts engendrés pourra être exigé sans préjuger des poursuites disciplinaires susceptibles d'être engagées.

3.11.Applications WEB et Logiciels

L'usage d'applications et logiciels non validés par la DMSI représente un risque important en matière de sécurité, de conformité réglementaire et de protection des données. À ce titre, il est strictement interdit :

- d'installer toute application (qu'elle soit payante ou gratuite) qui n'a pas été préalablement validée par la DMSI ;
- de souscrire au nom de la collectivité à une licence, sans avoir au préalable échangé avec la DMSI afin d'évaluer son adéquation avec les exigences de sécurité, de protection des données et de conformité aux réglementations en vigueur ainsi que l'alignement avec les choix stratégiques.

En cas de besoin d'un nouvel outil ou service en ligne, il est impératif de se rapprocher de la DMSI afin d'évaluer les solutions adaptées et sécurisées.

> **⃠ Limite**
>
> Il est impératif d'utiliser votre messagerie professionnelle pour accéder aux services en ligne, sauf dans le cas d'un « abonnement souscrit à titre individuel » (voir article 4.4).

3.12.Badges électroniques

Les badges électroniques sont utilisés pour sécuriser et contrôler l'accès aux locaux, aux équipements et à certains services spécifiques (parkings, télépéage, points d'apports collectifs, etc.). Leur utilisation est strictement encadrée afin d'assurer la sécurité des biens, des infrastructures et des informations.

3.12.1.Badges personnels

Les badges personnels permettent d'accéder à différents services et équipements selon les autorisations accordées par l'organisation. Ces badges nominatifs sont strictement personnels et ne doivent en aucun cas être prêtés ou partagés.

En outre, il est interdit d'utiliser son badge pour permettre l'accès à une personne non habilitée.

Tout badge perdu ou volé doit être signalé immédiatement au service vous l'ayant attribué.

Le badge doit être rendu en cas de départ, de fin de mission ou d'évolution des droits d'accès.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

3.12.2.Badges liés aux équipements

Certains badges permettent l'accès à des services dédiés comme par exemple le stationnement, le télépéage, ou les points d'apport volontaire.

Ces badges sont attribués selon des critères définis et ne doivent être utilisés que par les équipes ou véhicules autorisés.

Toute perte, vol ou anomalie d'utilisation doit être immédiatement signalé au service compétent.

Un badge lié à un service doit être restitué dès que son usage ou son absence d'usage ne remplit plus les conditions d'attribution.

3.13.Signature électronique et certificat

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

Cet usage est encadré afin de garantir l'authenticité, l'intégrité et la valeur légale des documents signés. Ainsi :

- toute signature électronique engageant l'organisation doit être réalisée avec un certificat délivré ou validé par la collectivité ;
- chaque utilisateur est responsable de la protection de son certificat et ne doit en aucun cas partager ses clés ou identifiants ;
- toute anomalie ou suspicion de compromission doit être signalée immédiatement à la DMSI ;
- les certificats seront révoqués lorsque leur utilisateur quitte la collectivité ou ne dispose plus de l'habilitation à l'utiliser.

> **⃠ Limite**
>
> Certains fournisseurs imposent l'utilisation de leur propre système de signature électronique. Dans ce cas, il convient de respecter leur processus tout en veillant à respecter autant que possible les exigences de sécurité de la collectivité.

3.14.Messagerie électronique

La collectivité met à disposition de ses utilisateurs qui le requiérent une messagerie électronique, destinée à un usage professionnel. Ces services sont paramétrés et administrés à cet effet.

Les règles générales d'utilisation :

- l'auteur doit s'identifier en faisant figurer en bas du message son nom, sa fonction et son service, éventuellement son numéro de téléphone. Le modèle de signature mis à disposition et intégré automatiquement aux messages doit ainsi être utilisé par défaut.
- la transmission d'informations par la messagerie doit respecter les procédures internes de contrôle, de validation, d'autorisation.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

- il est recommandé de vérifier la liste des destinataires avant l'envoi de tout message et d'utiliser la fonction copie cachée (Cci) afin de ne pas rendre le contenu de ces listes accessibles à tous.
- pour les transmissions de fichiers, il est recommandé de communiquer le chemin d'accès au fichier sur le réseau ou cloud.sbaa.fr dans son message, plutôt que d'envoyer le fichier en pièce jointe.
- il est recommandé de supprimer rapidement les courriels sans valeur professionnelle et juridique pertinente ainsi que les courriels contenant des données à caractère personnel. Si des logiciels « courrier » sont mis à disposition par la collectivité, leur usage doit être privilégié pour les courriers à valeur probante.
- les boîtes de messagerie ne doivent pas être considérées comme des espaces de stockage.

Engagement vis-à-vis des tiers

Un message électronique peut être une preuve ou un début de preuve. Ainsi, en matière commerciale, une preuve peut être apportée par tous les moyens possibles et il y a contrat dès lors que les parties ont donné leur accord sur la chose et sur le prix.

Il est donc rappelé que toutes les recommandations concernant les échanges écrits avec des tiers s'appliquent à la messagerie. Il est donc obligatoire de transmettre pour validation à un supérieur hiérarchique tout message qui aurait valeur contractuelle ou qui serait l'expression d'une décision administrative.

Utilisation de la messagerie électronique à des fins personnelles

Tout message reçu ou envoyé depuis le poste de travail mis à disposition de l'utilisateur est présumé professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée si elle est nécessaire pour des raisons de vie courante ou familiale et n'affecte pas le trafic normal de la messagerie professionnelle.

L'usage du mail professionnel pour créer des comptes sur des applications à vocation privée (réseau social, site commerçant, site de rencontre, etc.) est interdit.

Pour bénéficier du droit au respect de la vie privée et du secret des correspondances, un message personnel doit :

- comporter la mention « Privé », « Perso », « Personnel » ou « Droit syndical » au début de l'objet et, idéalement, le destinataire doit être informé de cet usage ;
- supprimer la signature identifiant la collectivité.

Enfin, les messages privés doivent être rangés dans un répertoire dédié portant la mention « Privé », « Perso », « Personnel » ou « Droit syndical ».

Traçabilité et Respect de la Vie Privée dans les Échanges Numériques

Toute activité numérique, comme l'utilisation de la messagerie électronique, laisse des traces et est nécessairement mémorisée. Ainsi, pour des raisons de sécurité, d'organisation ou de gestion de l'encombrement du réseau, la DMSI peut utiliser des dispositifs d'analyse de messages ou des dispositifs visant à limiter la taille ou le volume des messages échangés.

La mise en place de ces dispositifs n'ayant pas pour objet le contrôle individuel des utilisateurs, le principe de la confidentialité des messages sera respecté dans les termes indiqués dans le « RÈGLEMENT INTÉRIEUR DE L'USAGE DES SYSTÈMES D'INFORMATION - ADMINISTRATEUR », Chapitre : « Obligation de confidentialité et devoir général de discrétion».

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

4.Moyens destinés à assurer la sécurité informatique

La collectivité met en œuvre des systèmes destinés à assurer la protection contre les cyberattaques et les mauvais usages des ressources. Ces mesures doivent être complétées par une hygiène de ses utilisateurs. Ce chapitre vous les détaille.

4.1.Compte « utilisateur » et mot de passe

Chaque utilisateur du réseau informatique se voit attribuer un ou plusieurs comptes auxquels sont associés des identifiants (logins) et des mots de passe. L'utilisateur est responsable de ses comptes et de leur utilisation dans les termes ci-après.

La construction des mots de passe doit respecter les points suivants :

- la longueur minimale d'un mot de passe doit être de **12 caractères ;**
- le mot de passe **ne doit pas contenir de données personnelles de l'utilisateur** ;
- le mot de passe **ne doit pas contenir une référence aux collectivités ou aux départements ;**
- le mot de passe **doit être différent des derniers mots de passe utilisés**.

Il doit également respecter au moins trois des critères suivants :

- contenir des caractères minuscules ;
- contenir des caractères majuscules ;
- contenir des chiffres ;
- contenir des caractères spéciaux.

L'utilisateur ne doit pas utiliser les mêmes mots de passe dans la sphère personnelle et professionnelle et, dès que possible, choisir un mot de passe différent par système et/ou application. Les mots de passe doivent respecter les consignes de sécurité concernant leur longueur et leur complexité, et ne pas pouvoir être devinés facilement.

Les mots de passe ne doivent, en aucun cas, être notés, gardés au bureau ou stockés sous quelque forme que ce soit, excepté dans les solutions sécurisées développées à cette fin (coffre-fort de mots de passe validé par la DMSI). En cas de doute ou de notification sur la confidentialité d'un mot de passe, l'utilisateur doit lancer la procédure de réinitialisation dans les meilleurs délais.

> **Mémo**
>
> Tout nouveau mot de passe que je crée doit être différent.
>
> Si j'ai plusieurs mots de passe à mémoriser, j'utilise le coffre fort de mot de passe de la collectivité.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

4.2.Dispositifs de prévention des virus informatiques

La DMSI met en œuvre un système antivirus contrôlant les flux externes (Internet) et internes sur le réseau, qui intercepte et élimine les virus informatiques.

Néanmoins, afin de limiter les risques de diffusion de ces virus, il est strictement interdit :

- d'introduire des clés USB, disques venant de sources externes, sans l'accord préalable de la DMSI ;
- de connecter en USB à son poste informatique des équipements personnels (y compris pour le charger) : smartphones, tablettes, lecteurs MP3, etc.
- d'installer des logiciels externes sans l'accord préalable de la DMSI.

> 💡 **Conseil**
>
> Si j'ai besoin de charger mon smartphone personnel durant mon travail, je prévois un chargeur ou une batterie externe.

Il convient aussi de se méfier des fichiers transmis par messagerie, qui ont un caractère suspect ou provenant d'expéditeurs inconnus (cf. risques liés à la messagerie électronique ci-après). En cas de doute, vous devez vous adresser à la DMSI.

En cas de fonctionnement inhabituel de son poste informatique (lenteur du système et/ou du réseau, ouvertures de fenêtres non sollicitées, etc.) il convient de prévenir la DMSI.

> ⃠ **Limite**
>
> En cas de virus informatique résilient ou de crise majeure, le principe de précaution prévaudra et la DMSI ne reprendra pas les informations contenues sur les postes de travail avant réinitialisation du poste. Il est du devoir des utilisateurs d'enregistrer leurs fichiers sur le réseau au quotidien.
>
> La DMSI se réserve le droit de bloquer les ports USB et le réseau avant notification de l'utilisateur.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

4.3.Prévention des risques liés à la messagerie électronique / Règles relatives à la sécurité de la messagerie

La messagerie est l'un des premiers vecteurs de propagation des virus et de «phishing» (technique utilisée par des escrocs pour collecter des données personnelles). Il est en effet très simple de diffuser par email un fichier attaché contenant un virus, ou un lien Internet pour inciter à télécharger un programme infecté.

4.3.1.Règles relatives à la sécurité des services de messagerie

L'utilisateur doit obligatoirement utiliser en l'état les services de messagerie installés et configurés par la DMSI. À ce titre, l'utilisateur s'interdit de modifier les paramètres de sécurité.

L'utilisateur s'engage à ne pas utiliser, pour ses usages professionnels, des services de messagerie ou de partage et/ou stockage de données autres que ceux mis à disposition ou conseillés par la DMSI (ex. une messagerie personnelle Gmail, Yahoo, etc., un service de stockage cloud non maîtrisé par la DMSI tel que Dropbox, un service de transfert de fichiers tel que WeTransfer).

L'utilisateur a le droit de transférer des messages professionnels vers une autre messagerie personnelle dans le but légitime de préserver ses droits ou de fournir une preuve en sa faveur. Tout autre transfert de message relevant de la propriété intellectuelle de la collectivité est interdit sauf si l'information est de nature publique.

Pour les agents cette mise en œuvre devra faire l'objet d'une dérogation motivée et validée par le supérieur hiérarchique. Enfin, afin de prévenir des risques d'usurpation d'identité, il est impératif d'utiliser exclusivement la messagerie de la collectivité lors de l'envoi d'emails dans le cadre de leurs fonctions.

Pour les élus et les responsables syndicaux, la mise en œuvre d'un transfert automatique des mails vers une boite d'élu ou d'organisation syndicale est tolérée, mais déconseillée.

4.3.2.Règles relatives à la protection contre l'hameçonnage et la fraude

L'utilisateur doit éviter, autant que faire se peut, de publier son adresse électronique professionnelle sur Internet (ex. publication sur des blogs ou des profils de réseaux sociaux).

L'utilisateur doit faire preuve d'une vigilance accrue en cas de réception d'un message inhabituel ou douteux en provenance d'un expéditeur inconnu, présentant une syntaxe approximative, contenant des liens vers des sites et/ou des pièces jointes non sollicitées, demandant d'effectuer des actions inhabituelles ou ayant un caractère d'urgence. Lorsque l'utilisateur pense avoir reçu un tel message, il n'y répond pas et le signale immédiatement à la DMSI.

L'utilisateur ne doit cliquer sur un lien hypertexte contenu dans un message que lorsqu'il estime avoir « toute confiance » dans l'expéditeur et seulement après avoir vérifié la syntaxe du lien hypertexte. Si ce lien le dirige sur un site qui lui demande une authentification, l'utilisateur doit redoubler de vigilance, et contrôler l'adresse « réelle » du site cible avant de saisir ses identifiants. Si l'utilisateur a le moindre doute, il doit contacter sans délai la DMSI.

En raison des risques d'usurpation d'une adresse de messagerie, l'utilisateur doit faire preuve de discernement en cas de réception d'un message électronique « a priori » en provenance d'un responsable ou d'un tiers connu, lui demandant d'effectuer des actions inhabituelles ou non conformes aux procédures internes. Dans ce cas, l'utilisateur doit vérifier verbalement auprès de cette personne le bien-fondé de l'action par un second canal (appel téléphonique, échange dans son bureau, etc.).

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

4.4.Utilisation d'Internet

L'utilisateur doit avoir un usage professionnel et raisonnable des services Internet mis à sa disposition. Il doit notamment respecter les préconisations de nos collectivités en matière de sécurité informatique, ainsi que la législation en vigueur, notamment les dispositions relatives à la propriété intellectuelle et aux publications portant atteinte à la dignité de la personne humaine.

L'usage d'Internet pour les raisons suivantes est strictement interdit :

- la consultation des sites à caractère pornographique, xénophobe, terroriste, et toutes consultations de sites pouvant engager la responsabilité pénale de leurs créateurs et/ou utilisateurs ;
- la participation à des jeux d'argent ou de hasard, légaux ou illégaux ;
- l'accès à des sites ou services pouvant surcharger Internet et le réseau de nos collectivités ;
- pour des utilisations susceptibles d'engager la responsabilité civile ou pénale de l'utilisateur et/ou de la collectivité incluant les usages pouvant nuire à l'image ou à la réputation d'une autre personne ou de nos collectivités.

L'utilisateur doit être vigilant quant à l'utilisation de plateformes externes disponibles sur Internet, qui peuvent comporter des failles en matière de sécurité et de protection des données. Il doit donc privilégier l'utilisation d'outils préconisés par la DMSI. Si l'utilisateur souhaite utiliser d'autres plateformes, il doit demander au préalable l'avis de la DMSI.

L'accès à des outils et/ou sites proscrits par la DMSI, en utilisant d'autres moyens de connexion (Wi-Fi public, partage de connexion via mobile) pour un usage dans le contexte professionnel, est interdit.

Il est accordé une tolérance à l'accès à des sites Internet à des fins personnelles. Elle est permise dès lors qu'elle reste raisonnable, c'est-à-dire limitée dans sa fréquence, sa durée et qu'elle ne nuit pas au bon fonctionnement des services.

L'usage, à des fins professionnelles, d'un abonnement à un service en ligne (IA, correction orthographique, etc.) souscrit à titre individuel est toléré uniquement si toutes les conditions suivantes sont strictement respectées :

- vérifier que les conditions d'utilisation du fournisseur autorisent explicitement un usage professionnel individuel. L'utilisateur demeure seul responsable en cas de non-respect ;
- désactiver l'historique des échanges (chat history ou équivalent) afin d'éviter la mémorisation automatique des données ;
- conserver le compte strictement personnel, sans utilisation collective, familiale, ni intégration dans un produit ou service externe ;
- accepter qu'un contrôle encadré du compte puisse être demandé en cas d'incident de sécurité, de réquisition judiciaire ou d'enquête interne, afin de vérifier la conformité et la sécurité ;
- ne saisir, partager ou traiter aucune donnée personnelle, confidentielle, protégée par le secret des affaires ou relevant de la propriété de la collectivité.

Mémo

La liste des applications et services internet autorisés est disponible sur les intranets

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

4.5.Accès aux salles serveurs et baies techniques

L'accès aux salles serveurs et baies techniques étant restreint, toute personne qui désire y accéder est invitée à demander l'autorisation à la DMSI.

4.6.Règles relatives à la protection physique

4.6.1.Prendre soin de son matériel et ne pas l'exposer au vol

L'utilisateur est responsable de la sécurité physique des équipements qui lui sont confiés par la collectivité dans le cadre de sa mission. Dans ce cadre, l'utilisateur veille à avoir une utilisation respectueuse de ceux-ci (ex. éviter les chocs, ne pas manipuler de liquides à proximité, placer le matériel dans un lieu sûr et stable) et s'engage à prendre les mesures adaptées pour réduire les risques de casse, perte ou vol

4.6.2.Principe du bureau propre

A la fin de son travail, l'utilisateur s'engage à ne laisser en vue sur son bureau de travail, aucun actif important ou ayant de la valeur (téléphones portables, mot de passe, documents confidentiels et/ou sensibles, etc.).

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

5.Droits et devoirs des utilisateurs

Les utilisateurs des Systèmes d'Information de la collectivité disposent de droits. Ces droits ne pouvant prévaloir sur la sécurité de nos systèmes ni au bon usage de l'argent public. Leurs limites sont précisées dans les chapitres suivants.

5.1.Droit à la déconnexion

Dans le cadre de notre engagement envers le bien-être et l'équilibre entre vie professionnelle et vie personnelle des agents, la collectivité reconnaît et promeut le droit à la déconnexion. Ce droit permet à chaque agent de ne pas être joignable en dehors de ses horaires de travail, sauf en cas d'urgence clairement définie. Il est essentiel de respecter les plages de repos et de déconnexion pour prévenir les risques de surcharge de travail et de stress. Les outils numériques doivent être utilisés de manière responsable, en veillant à ne pas empiéter sur le temps personnel des agents. Des formations et des sensibilisations seront régulièrement proposées pour encourager une utilisation saine et équilibrée des technologies de l'information et de la communication.

Mémo

Le droit à la déconnexion vous autorise à :

- éviter l'enchaînement de réunions tout au long de la journée ;
- définir une heure de déconnexion en utilisant un réveil ou une alerte ;
- mettre en silencieux ou désactiver les notifications de votre smartphone en dehors des heures de travail ou d'astreinte ;
- programmer l'envoi de vos emails pour le lendemain ;
- laisser vos équipements au bureau en fin de journée, hors contexte de mobilité ou d'obligation de service ;
- Discuter avec votre encadrant des difficultés que vous rencontrez.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

5.2.Tolérance de l'utilisation à des fins privées

L'utilisation des moyens informatiques et de communication à des fins privées est tolérée de manière occasionnelle pour répondre aux nécessités de la vie courante (« vie privée résiduelle »), sous réserve que cet usage :

- n'affecte pas les conditions d'accès, le bon fonctionnement ou la sécurité des services concernés ;
- ne mette pas en cause la productivité de l'utilisateur dans l'accomplissement de ses missions professionnelles ni celles de ses collègues ;
- soit fait de manière responsable, éthique et respectueuse d'autrui afin qu'il ne puisse en aucun cas nuire aux intérêts ni à l'image de la collectivité ;
- n'occasionne pas de frais et/ou d'investissements supplémentaires ;
- reste conforme au présent règlement, aux dispositions légales, au contrat de travail et aux règles fixées par la collectivité.

> **⃠ Limite**
>
> L'usage des moyens informatiques et de communication de la collectivité dans le cadre de la « vie privée résiduelle » ne permet pas l'usage dans un cadre associatif ou pour une activité extraprofessionnelle.

5.3. En cas d'absence d'un utilisateur

5.3.1.Accès aux données

L'utilisateur et sa hiérarchie doivent s'organiser pour permettre la continuité d'accès aux données et logiciels en l'absence d'un utilisateur.

Exceptionnellement, en l'absence d'un utilisateur (par exemple pour arrêt maladie), l'employeur est en droit d'accéder à son poste de travail, à sa messagerie professionnelle et aux courriels adressés par l'utilisateur à l'aide des outils informatiques mis à sa disposition.

Cette présomption d'accès libre ne vaut que pour les messages identifiés comme étant professionnels. Si l'employeur s'aperçoit qu'il a accédé à un message privé, il ne pourra s'en servir dans le cadre d'une quelconque procédure à l'encontre de l'utilisateur. Sauf s'il mettait en évidence un délit pour lequel l'employeur serait dans l'obligation d'en référer au législateur.

Le droit d'accès aux données n'autorise pas l'employeur, ni l'administrateur à envoyer un mail en se faisant passer pour l'utilisateur ; à supprimer une correspondance (sauf du fait du mécanisme automatique de suppression des boites mail au départ de l'utilisateur).

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

5.3.2.Information en cas d'absence

En cas d'absence, les utilisateurs doivent informer leurs collègues en configurant un message d'absence automatique dans leur messagerie électronique. Ce message doit indiquer la date de retour si possible, et les coordonnées d'une personne à contacter en cas d'urgence.

Pour les partenaires externes, il est recommandé de limiter la communication de l'absence aux contacts essentiels et de confiance, afin de ne pas divulguer d'informations pouvant être exploitées par des acteurs malveillants. Les messages d'absence destinés aux partenaires doivent être rédigés de manière à ne pas révéler de détails sensibles sur la durée ou la nature de l'absence.

En complément, les utilisateurs doivent activer le renvoi d'appels sur leurs lignes téléphoniques professionnelles vers un collègue ou un service approprié, afin de garantir la continuité du service et la prise en charge des demandes urgentes.

Pour des raisons de service, en l'absence d'un utilisateur (par exemple pour arrêt maladie ou départ), l'employeur est en droit de paramétrer ce message d'absence ou le renvoi d'appels sur validation du responsable hiérarchique de l'agent concerné.

Ces mesures permettent de maintenir une communication fluide et de répondre efficacement aux besoins des interlocuteurs pendant les périodes d'absence.

5.3.3.Désactivation des comptes et restitution du matériel

En cas d'absence prolongée, la restitution du matériel ainsi que la désactivation des comptes d'accès pourront avoir lieu si elles résultent d'un besoin opérationnel ou d'un besoin de sécurité.

5.4.En cas de départ d'un utilisateur

L'utilisateur doit restituer les ressources et le matériel informatiques qui lui ont été alloués, ainsi que les données professionnelles associées, en cas de départ de la collectivité ou sur demande de l'autorité territoriale.

Avant son départ de la collectivité, il doit préalablement effacer ses fichiers et données privées. Toute copie de documents professionnels doit être autorisée par le supérieur hiérarchique et portée à la connaissance du Responsable de la Sécurité des Systèmes d'Information (des modèles de demande d'exfiltration de données sont disponibles sur vos intranets).

Concernant le matériel, le supérieur hiérarchique doit organiser la restitution de l'équipement.

Les comptes de l'utilisateur, ses données personnelles et ses ressources dédiées sur le réseau local sont supprimés dans un délai d'un mois après son départ de la collectivité. Concernant la messagerie, celle-ci reste en service pendant un mois après le départ de l'utilisateur. Celui-ci doit mettre en place un message informant ses correspondants de sa cessation d'activité et indiquant, le cas échéant, les coordonnées de son remplaçant.

Concernant les ressources de l'utilisateur sur le réseau de la collectivité, en fonction de l'intérêt des informations stockées, il peut soit les détruire, soit les enregistrer sous une ressource commune de service en vue d'en faire bénéficier son successeur ou d'autres agents du service. Il appartient au supérieur hiérarchique de veiller à la bonne conservation de ces données, dans une logique de continuité d'activité et de partage des connaissances au sein du service.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

5.5.En cas de perte ou vol

En cas de perte ou de vol d'un matériel confié à l'utilisateur (poste de travail, téléphone, clé USB, etc.), celui-ci doit prendre contact avec la DMSI et informer son supérieur hiérarchique dans les plus brefs délais, afin de procéder au blocage de l'appareil et d'engager toutes les démarches nécessaires (plaintes, remplacement du téléphone, déclaration CNIL, etc.).

5.6.Le droit syndical

L'utilisation de la messagerie, de l'intranet et d'Internet est autorisée aux organisations syndicales représentatives des personnels sous réserve du respect des règles du présent règlement.

En outre, l'utilisation de la messagerie de la collectivité pour des communications à grande échelle leur est autorisée à condition :

- de ne diffuser que des informations et des données d'intérêt général ou d'origine syndicale ;
- de s'abstenir de toute mise en cause personnelle ou nominative ;
- que les diffusions soient limitées au personnel de la collectivité où l'organisation syndicale est représentative ;
- que les destinataires soient informés de la possibilité de se désabonner et de s'opposer à la réception de ces messages.

En cas de manquement à ces règles, ou du non respect du présent règlement, les organisations syndicales représentatives, s'exposent à une suspension proportionnée des accès (messagerie, intranet et Internet).

Tous les fichiers présents dans un dossier « Droit syndical » bénéficient de la protection liée au droit syndical. Il en est de même de tout message qui comportera la mention « Droit syndical » en objet.

5.7.Le droit associatif

L'utilisation du système d'information, de la messagerie, de l'intranet et d'Internet est autorisée pour les organisations associatives œuvrant dans l'intérêt du personnel (amicales), sous réserve du respect des règles énoncées dans le présent règlement.

En outre, l'utilisation de la messagerie leur est autorisée uniquement pour :

- Les échanges internes entre membres du conseil d'administration
- Les échanges à destination des partenaires
- La communication aux agents membres d'informations essentielles au bon déroulement des actions de l'association : annonces d'actions et d'animations à destination des membres, dates essentielles (ex : assemblée générale), modifications/ajustements des actions, animations, réunions, etc.

Sauf dispositif technique mis à disposition de l'association par la collectivité (Ex : Page d'intranet d'actualité). Les informations destinées à l'ensemble des agents (promotion des actions et des animations, dates essentielles, réunions, ...) sont à transmettre à la Direction Communication pour mise en ligne sur l'intranet. Elles doivent répondre aux principes d'un contenu neutre et purement informatif, sans prise de position. Les éléments transmis sont relus et adaptés au besoin.

En cas de manquements à ces règles, ou du non respect du présent règlement, l'association, s'expose à une suspension proportionnée des accès (système d'information, messagerie, intranet et Internet).

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

6.Obligation en matière de protection des données

Les données de notre collectivité ainsi que son image sont des éléments de valeur qu'il convient de défendre et de manipuler avec attention. Ce chapitre détaille ces éléments.

6.1.Règles d'accès et de stockage des données professionnelles

Les 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 des supports 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.

Les utilisateurs s'engagent par ailleurs à ne pas prendre connaissance d'informations appartenant 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 l'enregistrement de données à caractère personnel et confidentiel doit être effectué uniquement sur les répertoires placés sous responsabilité du service ou de la direction.

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

6.2.Protection des données

6.2.1.Responsabilité des utilisateurs

Un utilisateur qui accède ou reçoit des données à caractère personnel, qu'il s'agisse de données relatives aux collaborateurs de la collectivité ou à des tiers (usagers, partenaires, candidats, etc.), s'engage à respecter strictement la réglementation applicable et les consignes associées au traitement de ces données selon les lois nationales en vigueur (Règlement Général sur la Protection des Données « RGPD » / Règl. UE 2016/679).

L'utilisateur devra solliciter le Délégué à la Protection des Données de la collectivité ou le service Juridique, avant toute mise en œuvre de nouveaux traitements de données personnelles, afin de s'assurer du respect de ses obligations.

Si l'utilisateur détecte une violation de données à caractère personnel ou une non-réponse à un droit, il devra prévenir le Délégué à la Protection des Données de la collectivité ou le service Juridique.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

6.2.2.Droits des utilisateurs

Dans le cadre de l'utilisation des outils informatiques mis à disposition par la collectivité, la DMSI sera amenée à traiter des données à caractère personnel relatives aux utilisateurs. Ces données sont nécessaires dans le cadre de la mise à disposition d'outils informatiques (suivi et maintenance du parc informatique, gestion des annuaires informatiques, mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux, gestion de la messagerie électronique, etc.). En complément et dans le cadre de notre engagement à assurer la sécurité et l'intégrité de nos systèmes informatiques, nous vous informons que certaines données personnelles, telles que les adresses IP, peuvent être traitées pour des finalités spécifiques liées à la sécurité informatique. Ce traitement est fondé sur notre intérêt légitime à protéger nos réseaux et nos systèmes contre les accès non autorisés, les intrusions, les fraudes, et autres menaces potentielles. Les données collectées seront utilisées exclusivement dans ce cadre et ne seront pas exploitées à d'autres fins sans votre consentement explicite. Les données sont conservées pendant toute la durée de présence de l'utilisateur au sein de la collectivité puis seront supprimées dans un délai de 6 mois à compter de son départ.

Les destinataires des données sont : la DMSI.

Les utilisateurs dont le traitement des données à caractère personnel est soumis au RGPD sont informés qu'ils disposent d'un droit d'accès et de rectification relatif à l'ensemble de leurs données à caractère personnel les concernant, d'un droit d'opposition pour motif légitime, d'un droit d'effacement, de limitation du traitement. L'utilisateur peut exercer ses droits en contactant le Délégué à la Protection des Données de la collectivité.

Si l'utilisateur est victime d'une violation de données à caractère personnel le concernant, il peut prévenir le Délégué à la Protection des Données de la collectivité ou le service Juridique.

> **Mémo**
>
> Vous trouverez les coordonnées du responsable de traitement ou, le cas échéant, de votre délégué à la protection des données sur les sites de votre collectivité

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

6.3.Utilisation des solutions d'intelligence artificielle générative

Dans le cadre de l'utilisation de tout système d'intelligence artificielle générative, les utilisateurs s'engagent expressément à ne pas communiquer ou mentionner :

- de données personnelles liées à des personnes physiques d'une part (nom, prénom, adresse, numéro de téléphone, identifiants, informations financières, données de santé, etc.),
- de données confidentielles liées aux projets de votre collectivité,
- de données confidentielles liées à l'un de nos partenaires ou fournisseurs (données financières, stratégiques),
- de données sensibles relatives aux marchés publics et d'une manière générale couvertes par le secret des affaires.

Les utilisateurs doivent veiller à ce que toutes les informations échangées avec un système d'Intelligence artificielle externe respectent les obligations de confidentialité et de protection des données en vigueur, conformément à la réglementation applicable, notamment le Règlement Général sur la Protection des Données (RGPD). Toute violation de cette clause pourra entraîner des mesures disciplinaires, conformément à la politique interne de l'organisation.

Cette interdiction vise à protéger la vie privée des individus et la confidentialité des opérations de votre collectivité et à garantir que l'usage de l'outil se fait dans un cadre sécurisé et conforme aux normes de confidentialité en vigueur.

6.4.Utilisation des médias sociaux

Les médias sociaux regroupent tous les sites internet, applications ou plateformes qui permettent aux utilisateurs de créer du contenu, de l'organiser, de le modifier ou de le commenter. Outre les réseaux sociaux, ils peuvent prendre des formes extrêmement variées allant de la messagerie électronique à la diffusion d'actualités en passant par le partage de contenu (texte, photo, vidéo, musique), le commerce en ligne ou les plateformes de jeux (selon la définition du « web 2.0 »).

Tous les espaces virtuels où l'utilisateur peut être amené à faire un commentaire, interagir ou laisser son empreinte numérique sont concernés.

Utilisés à bon escient, ces outils de communication ouvrent des possibilités nouvelles de contact direct entre l'usager et l'institution. Néanmoins, la facilité d'accès, l'illusion d'anonymat et le sentiment d'impunité qui en découle, la mauvaise connaissance des paramètres de confidentialité, peuvent mettre à mal l'obligation de réserve à laquelle chaque agent est tenu, et l'exposer à des sanctions.

Les médias sociaux doivent ainsi être utilisés avec discernement et engagent chacun à respecter des règles de communication.

6.4.1.Les précautions à prendre lors de l'utilisation des réseaux sociaux

Les plateformes sociales sont de véritables espaces publics, visibles et consultables par tous. Tout le monde peut propager vos idées en republiant un contenu écrit, vidéo ou audio instantanément.

Vos conversations, personnelles ou professionnelles, peuvent être diffusées partout sans votre accord. Vous êtes donc impliqué personnellement sur tout ce que vous publiez ou retransmettez (partage, «like», «retweet», commentaire, etc.).

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

Les informations que vous postez sont indexées par les moteurs de recherche. Elles laissent des traces durables qui peuvent vous suivre tout au long de votre vie, si vous n'agissez pas à temps.

> **Mémo**
>
> Prenez quelques minutes de réflexion avant de publier un contenu.

Même si ces réseaux sont des lieux de liberté d'expression, restez prudents : exprimez-vous en toute connaissance des sujets traités.

Soyez respectueux des autres et de leur vie privée. Ne diffusez pas d'information ou ne citez pas de personnes sans leur accord. Ne photographiez pas des personnes sans leur autorisation

6.5.Propriété intellectuelle

L'utilisation des ressources informatiques implique le respect de la législation applicable en matière de propriété intellectuelle.

L'utilisateur s'engage à ne pas utiliser l'accès internet et les ressources de la collectivité mises à sa disposition à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin (tels que des textes, images, logos, dessins, photographies, œuvres musicales, œuvres audiovisuelles, logiciels et jeux, etc.) sans autorisation. Le fait qu'un contenu, un document, une photo ou un article soit publié en ligne ne signifie pas que ce contenu est libre de droits.

L'utilisateur doit veiller à ne pas utiliser les logiciels mis à disposition en dehors des conditions d'utilisation communiquées par l'éditeur.

> **Mémo**
>
> En cas de doute sur un aspect législatif, le service juridique de votre collectivité peut être sollicité.

6.6.Règles de déontologie et d'éthique

L'agent public (fonctionnaire ou contractuel) de la collectivité est soumis aux droits et obligations des agents publics tels que définis par la loi n°83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires et la loi n°84-53 du 26 janvier 1984 modifiée relative à la fonction publique territoriale. Ainsi, il se doit de respecter ses obligations de réserve, de discrétion et de secret professionnel, par l'usage des ressources informatiques mises à sa disposition par nos collectivités.

L'agent de droit privé est soumis aux mêmes obligations dès lors qu'il concoure à l'exercice d'une mission de service public.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

Ces obligations valent également dans le cadre de l'usage d'outils informatiques personnels, et en dehors des heures de travail de l'utilisateur (publications sur les réseaux sociaux ou sur des forums de discussion à titre privé par exemple).

L'utilisateur disposant du statut d'élu local, par l'usage des ressources informatiques mises à sa disposition par la collectivité, est soumis aux dispositions de la charte de l'élu local, figurant à l'article L1111-1-1 du Code Général des Collectivités Territoriales. Conformément à cet article, l'élu doit « exercer ses fonctions avec impartialité, diligence, dignité, probité et intégrité ».

Ainsi, l'utilisateur ne doit en aucun cas porter atteinte à l'image de la collectivité et ne peut divulguer de données personnelles ou professionnelles, d'informations sensibles, confidentielles ou considérées comme stratégiques à des personnes non habilitées à les recevoir, sans l'accord de l'autorité territoriale.

À plus large spectre, il ne doit pas accéder à des informations pour lesquelles il n'a pas à en connaître dans le cadre de ses missions.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

7.Engagement de respect du Règlement et sanctions

Il est de la responsabilité de chaque utilisateur des Systèmes d'Information de nos collectivités de protéger les outils qui lui ont été confiés et les données auxquelles il a accès.

Tout utilisateur des Systèmes d'Information de la collectivité s'engage à respecter l'ensemble des principes, règles et obligations figurant dans le présent règlement. À défaut, il engage sa responsabilité. L'utilisateur fautif s'expose à un rappel des règles et à d'éventuelles sanctions de nature disciplinaire respectant une phase contradictoire, appropriées et proportionnées, sans préjuger des actions complémentaires pouvant être engagées à son encontre sur le plan civil et pénal.

Par ailleurs, si la survenance d'un événement préjudiciable au bon fonctionnement d'un SI est détectée, la collectivité pourra (le temps nécessaire à l'investigation et à la remise en condition de sécurité) restreindre ou suspendre l'accès aux moyens informatiques ou leur usage à l'utilisateur à l'origine d'un incident réel ou supposé.

En cas de doute quant à l'application des règles du présent règlement, l'utilisateur peut contacter la DMSI ou son Délégué à la protection des données ou son service des ressources humaines.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

8.Contrôle de ressources

Conformément à la loi, la collectivité est responsable de l'utilisation faite par les utilisateurs des ressources des Systèmes d'Information mis à leur disposition. La collectivité se réserve ainsi le droit d'analyser, de limiter et de contrôler l'utilisation des ressources matérielles et logicielles ainsi que les échanges effectués via son Système d'Information.

Les contrôles mis en œuvre par la collectivité sont réalisés par les administrateurs dans l'objectif de garantir le bon fonctionnement technique, la sécurité des Systèmes d'Information, et de préserver les intérêts de la collectivité.

Ainsi, des contrôles peuvent être effectués :

- de manière aléatoire ;
- dans le cadre d'audit de la sécurité de nos systèmes ;
- sur demande d'un supérieur hiérarchique ;
- en cas d'anomalie de facturation ;
- en cas d'alerte des services de police ;
- en cas de constat de dysfonctionnement dans l'activité d'un agent ;
- en cas d'encombrement d'un Système d'Information de la collectivité ;
- en cas d'attaque informatique.

Dans le cas de circonstances graves d'utilisations illégales ou non autorisées ou remettant en cause le bon fonctionnement d'un Système d'Information, la sécurité ou les intérêts de la collectivité, les membres de la DMSI pourront mettre en œuvre les actions de protection adaptées et/ou les corrections nécessaires jusqu'au retour à la normale, et informer la Direction Générale.

9.Numérique responsable

La collectivité promeut l'usage d'un numérique responsable en intégrant des pratiques durables et éthiques dans l'utilisation des technologies de l'information. Cela inclut la réduction de notre empreinte carbone numérique par l'optimisation de nos infrastructures et l'adoption de solutions technologiques éco-responsables. La collectivité encourage également la sensibilisation et la formation des agents aux enjeux environnementaux liés au numérique, afin de favoriser des comportements respectueux de l'environnement.

Chaque utilisateur a une responsabilité individuelle dans la mise en œuvre de cette démarche et doit veiller à suivre les conseils apportés par sa collectivité. Et, dans le cadre de nos engagements et des contraintes réglementaires pour un numérique responsable, la DMSI est seule responsable du choix du matériel fourni, qu'il soit neuf ou de réemploi, dès lors qu'il répond aux besoins opérationnels. Par conséquent, l'utilisateur ne peut exiger la fourniture d'un matériel neuf ou proposant des fonctionnalités superflues.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

10.Principaux textes de référence

- le règlement (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;
- la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- la loi n°78-17 du 06/01/78 dite « Informatique et liberté » modifiée par la loi n°2018-493 ;
- la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques ;
- la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
- la législation relative à la propriété intellectuelle ;
- la législation relative à la fraude informatique ;
- la législation en matière de transmission d'informations à caractère violent, pornographique ou de nature à porter gravement atteinte à la dignité humaine et à la diffusion de contenus illicites à caractère injurieux, diffamatoire, raciste, xénophobe, révisionniste et sexiste (articles 227-23 et 227-24 du code pénal et loi du 29 juillet 1881) ;
- le décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques ;
- la 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 ;
- les dispositions du code pénal relatives à la fraude informatique et aux atteintes aux droits de la personne et notamment les articles 226-1, 226-15 à 226-24, 321-1 à 323-7 ;
- l'ensemble des dispositions statutaires et notamment la 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 ;
- les dispositions du code du travail relatives à l'information préalable des salariés sur l'existence des moyens et dispositifs de contrôles mis en place, notamment les articles L. 121-8 et L. 432-2-1 ;
- la circulaire du 12 mars 1993 relative aux modalités de l'application de la loi "informatique et libertés" au secteur public ;
- le guide d'hygiène informatique - Agence nationale de la sécurité des systèmes d'information – Janvier 2017.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

Direction Mutualisée des Systèmes d'Information
assistanceinfo@sbaa.fr - 02 96 63 25 40

POLITIQUE - Règlement intérieur de l'usage des systèmes d'information à destination des administrateurs

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

Table des matières

Glossaire .....
Objet et champ d'application du règlement .....
Engagement de respect du règlement et sanctions .....
Droits de l'administrateur .....
- Droits d'intervention technique .....
- Données personnelles de l'administrateur .....

Devoir de l'administrateur .....
- Obligation de confidentialité et devoir général de discrétion .....
- Règles de sécurité .....
  - Incidents de sécurité .....
  - Protection des droits d'accès à privilèges .....
  - Utilisation des logiciels et équipements spécifiques .....
  - Continuité d'activité .....
  - Départ de l'administrateur .....
- Principes liés aux activités de contrôle .....
  - Principe de proportionnalité .....
  - Principe de transparence .....
  - Principe de loyauté .....

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

1.Glossaire

« Données personnelles » : Toute information se rapportant à une personne physique identifiée ou identifiable (directement ou indirectement) : nom, prénom, numéro de téléphone, numéro d'identification, données de localisation, identifiant en ligne, photographies, etc.

« Prestataire »: Toute personne physique ou organisme étranger à l'entreprise offrant des services/prestations et ayant un accès au système d'information.

« Personne non autorisée » : Toute personne, quel que soit son statut ou son niveau hiérarchique, ne disposant pas de l'autorisation explicite ou de la compétence requise pour intervenir dans le cadre d'une mission donnée.

« Responsable de la Sécurité des Systèmes d'Information » (RSSI) : Personne chargée du pilotage de la sécurité des Systèmes d'Information

« Système d'Information » : Ensemble organisé de ressources (matériels, logiciels, données et procédures) qui permet de traiter, stocker, présenter, détruire et diffuser de l'information, quelle que soit sa forme (électronique, imprimée, manuscrite, vocale, etc.).

« Utilisateur » : Toute personne autorisée à accéder, stocker, utiliser ou traiter des ressources d'un système d'information de la Collectivité quel que soit son statut (notamment agent de droit public ou privé, élu, personnel intérimaire, stagiaire, prestataire), ou sa localisation (au sein ou hors des locaux).

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

2.Objet et champ d'application du règlement

Le présent règlement a pour objectif de définir le rôle et les responsabilités des Administrateurs des Systèmes d'Information, en énonçant les principes, règles et obligations spécifiques qui leur sont applicables dans le cadre de l'exercice de leurs missions professionnelles. Il vient en complément du règlement intérieur de l'usage des systèmes d'information pour les utilisateurs, chaque administrateur étant également utilisateur de ces systèmes.

Un Administrateur est défini comme toute personne, quel que soit son statut (notamment agent de droit public ou privé, personnel intérimaire, élu, stagiaire, infogérant, consultant ou prestataire) ou sa localisation (au sein ou hors des locaux) qui a pour mission d'assurer le maintien en condition opérationnelle ou le paramétrage des composants des Systèmes d'Information de Saint-Brieuc Armor Agglomération, de la ville de Saint-Brieuc, de la ville de Ploufragan, du CIAS et de leurs satellites placés sous sa responsabilité (réseaux, composants de sécurité, applications, bases de données, postes de travail, flux de données, règles de gestion, etc.).

L'Administrateur peut ainsi réaliser différentes actions d'administration ou d'exploitation. Par exemple l'installation, la configuration, la maintenance, le support et l'évolution des ressources des Systèmes d'Information. Les personnes responsables du bon fonctionnement des applications métiers, et ayant de ce fait des droits de paramétrage sur les données et/ou les droits d'accès sont des Administrateurs.

Afin de conduire les actions quotidiennes afférentes à sa mission, l'Administrateur est doté de droits d'accès privilégiés sur les ressources d'un système d'Information sous sa responsabilité. Les risques associés à ces droits d'accès privilégiés peuvent être :

- La possibilité d'accéder à des informations dont il n'est pas destinataire, certaines étant confidentielles (bases de données, documents sur les postes de travail utilisateurs, etc.), à caractère personnel (courriels, fichiers personnels des utilisateurs, etc.) ou encore relatives aux activités des utilisateurs (données de connexion, etc.) ;
- La réalisation d'actions potentiellement dangereuses pour la sécurité des Systèmes d'Information : modification ou contournement des mécanismes de protection, création ou modification des comptes utilisateurs, destruction ou modification des fichiers, etc.

L'Administrateur joue ainsi un rôle de confiance, sa démarche doit être éthique et son action ne doit pas avoir une finalité personnelle non compatible avec ses missions professionnelles.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

3.Engagement de respect du règlement et sanctions

Tout administrateur s'engage à respecter l'ensemble des principes, règles et obligations énoncés dans le présent règlement. En cas de manquement, il engage sa responsabilité personnelle et s'expose à des sanctions disciplinaires, à un blocage immédiat de ses comptes, voire à des poursuites judiciaires conformément à la législation en vigueur.

Les administrateurs externes (consultants ou prestataires) sont également tenus de respecter l'ensemble des dispositions de ce règlement. En cas de non-respect, ils engagent leur responsabilité personnelle ainsi que celle de la société qui les emploie. Ils s'exposent alors à des poursuites judiciaires, au blocage de leurs comptes, ainsi que la suspension du contrat et des accès accordés à leur société.

En cas de doute quant à l'application des règles du présent règlement, l'Administrateur doit contacter le Responsable de la Sécurité des Systèmes d'Information.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

4.Droits de l'administrateur

Les administrateurs exercent leurs fonctions dans un cadre défini, qui garantit à la fois leur capacité d'actions et le respect de leurs droits en tant que personnes concernées par des traitements de données à caractère personnel.

4.1.Droits d'intervention technique

L'Administrateur peut prendre les dispositions qui lui semblent nécessaires afin d'assurer le bon fonctionnement et la sécurité des composants des Systèmes d'Information dans son périmètre de responsabilité. Il peut notamment effectuer les tâches suivantes, dans le cadre de procédures établies :

- isoler, arrêter ou reconfigurer des comptes utilisateurs, des équipements ou des applications informatiques pouvant compromettre la sécurité de l'ensemble des Systèmes d'Information ;
- procéder à des vérifications techniques sur des fichiers, des bases de données de journalisation ou de configuration, afin de déceler toute anomalie ou incident de sécurité qui pourrait porter atteinte au bon fonctionnement ou à la protection des Systèmes d'Information ;
- traiter (détection, analyse, éradication, filtrage, etc.) tous les flux informatiques présentant des risques potentiels de sécurité (virus, intrusion, utilisation d'un logiciel non autorisé, mail malveillant, etc.).

En cas de comportements anormaux identifiés, en lien avec l'activité des utilisateurs, l'Administrateur peut avoir à réaliser les actions suivantes, en conformité avec l'organisation et les procédures éventuellement en place :

- interruption prolongée d'un service ;
- interruption de toute tâche utilisateur, dans le cas où une utilisation excessive des ressources nuit au bon fonctionnement du système, après prise de contact avec l'utilisateur si applicable ;
- archivage, compression ou suppression des données excessivement volumineuses ou sans lien direct avec l'activité professionnelle (avec ou sans préavis si l'urgence de la situation le requiert) en cas de dégradation de service.

L'Administrateur se réfère au présent Règlement, au règlement intérieur de l'usage des systèmes d'information - utilisateur, à la fiche de poste et/ou au contrat de travail de l'agent ainsi qu'à la législation en vigueur pour fixer le cadre et les limites de ses interventions.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

4.2.Données personnelles de l'administrateur

Dans le cadre de l'administration des outils informatiques, nos services sont amenés à traiter des données relatives aux administrateurs. Ces données sont nécessaires dans le cadre du suivi des actions d'administration. Les administrateurs dont le traitement des données à caractère personnel est soumis au RGPD sont informés qu'ils disposent d'un droit d'accès et de rectification relatif à l'ensemble de leurs données à caractère personnel les concernant, d'un droit d'opposition pour motif légitime, d'un droit d'effacement et de limitation du traitement. L'administrateur peut exercer ses droits en contactant le Délégué à la Protection des Données de la collectivité.

Mémo

Si un éclairage juridique est nécessaire, l'administrateur peut solliciter les agents des services « Délégué à la Protection des Données », « Juridique », « Ressources Humaines », ou « Responsable de la Sécurité des Systèmes d'Information ».

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

5.Devoir de l'administrateur

L'administrateur a la possibilité d'accéder à des informations dont il n'est pas destinataire et d'opérer des actions potentiellement dangereuses pour la sécurité des Systèmes d'Information. Ce chapitre vise à préciser les obligations afférentes à son rôle.

5.1.Obligation de confidentialité et devoir général de discrétion

D'une manière générale, l'Administrateur est tenu de préserver la confidentialité des données auxquelles il a accès à l'occasion de sa mission, et de respecter la vie privée des personnes concernées ainsi que le secret des correspondances échangées au travers des Systèmes d'Information.

L'Administrateur est ainsi soumis à une obligation de confidentialité et de discrétion liée à ses activités, et dans ce cadre il s'engage durant et après son contrat à :

- ne pas consulter des informations des Systèmes d'Information auxquels il aurait accidentellement eu accès, ni d'y donner accès, en dehors du cadre de ses fonctions et/ou sur demande explicite de son responsable hiérarchique direct ou de son donneur d'ordre, dans le respect des procédures ;
- ne pas consulter des données personnelles des utilisateurs (signalées comme telles par l'utilisateur ou manifestement de nature « privée » ou « syndicale »), sauf :
    - ponctuellement, sur demande formalisée de l'utilisateur, ni d'autoriser quiconque à y accéder ;
    - cas particuliers prévus par la loi (par exemple, une enquête judiciaire) ;
    - habilitations formelles et légitimes préalablement déclarées comme indiqué dans la «RÈGLEMENT INTÉRIEUR DE L'USAGE DES SYSTÈMES D'INFORMATION - UTILISATEUR, Chapitre 5.2 : Tolérance de l'utilisation à des fins privées ».
- respecter ses engagements de confidentialité et de non-divulgation. Il ne doit pas utiliser les informations qu'il peut être amené à connaître dans le cadre de ses fonctions pour une autre finalité que la réalisation de ses fonctions ;
- ne pas accéder au poste de travail d'un utilisateur en cours d'usage sans son autorisation explicite, en particulier lors de l'utilisation d'un logiciel de contrôle à distance sur le poste de travail d'un utilisateur ;
- avertir le délégué à la protection des données lorsque l'incident de sécurité constitue une violation de données à caractère personnel.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

5.2.Règles de sécurité

L'Administrateur respecte strictement les règles de sécurité et les limites fixées à ses interventions, notamment :

- il n'abuse pas des droits d'accès privilégiés, et limite ses actions aux ressources des Systèmes d'Information sous sa responsabilité. En particulier, il ne modifie les configurations et les droits d'accès aux ressources que dans le respect des procédures d'administration ou d'exploitation préalablement définies ;
- il ne prend pas de consigne d'une personne non autorisée, quel que soit son niveau hiérarchique. Si une demande reçue paraît inappropriée ou non conforme aux règles de sécurité informatique, à la confidentialité des données ou à la déontologie, l'administrateur doit en informer son/sa responsable et/ou directeur.trice. Ils s'assureront que la demande est conforme avant d'autoriser par écrit sa réalisation. Au besoin, l'administrateur peut prendre conseil auprès du Responsable de la Sécurité des Systèmes d'Information ou de son Délégué à la Protection des Données ;
- il ne contourne pas les procédures de sécurité établies et, en particulier, il ne révise pas les droits qui lui ont été attribués ni ne désactive de sa propre initiative les mécanismes de traçabilité ou modifie les fichiers de journalisation qui permettent de définir les actions qui lui sont imputables ;
- il informe les usagers en cas de coupure de service programmée dans le cadre des procédures établies par son service ;
- il ne réalise aucune action pouvant impacter la sécurité des Systèmes d'Information sans demander l'autorisation du Responsable de la Sécurité des Systèmes d'Information ;
- il demande obligatoirement à un utilisateur de changer son mot de passe si pour une raison ou pour une autre il en avait connaissance ;
- il s'impose des mots de passe respectant les exigences des mots de passe utilisateur complétées par une longueur minimale de 16 caractères ; (Voir chapitre 4.1 du RÈGLEMENT INTÉRIEUR DE L'USAGE DES SYSTÈMES D'INFORMATION – UTILISATEUR) ;
- il ne stocke jamais des mots de passe en clair ou dans des logiciels avec une sécurité insuffisante (Fichiers, navigateurs, outils d'administration …), que ce soit pour ses propres comptes ou des comptes techniques. À ce titre, il peut utiliser le gestionnaire de mot de passe « https://secret.sisbaa.fr » ou Keepass DMSI.

Mémo

Si une mesure de sécurité ne peut être maintenue durablement en raison de la nécessité de garantir la continuité du service, il est nécessaire de consigner cette exception et d'obtenir l'approbation de son supérieur hiérarchique par le biais d'une demande de dérogation (le formulaire est accessible sur l'intranet).

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

5.2.1.Incidents de sécurité

L'administrateur doit informer sans délai son supérieur hiérarchique ou donneur d'ordre d'une faille ou d'un incident de sécurité qu'il aurait découvert ou dont il aurait pris connaissance. Il doit en outre préserver toutes les traces nécessaires à la résolution de l'incident et à toute investigation ultérieure, dans des conditions permettant de garantir leur valeur probante.

En synthèse, en tant qu'Administrateur, les réflexes suivants sont à avoir en cas d'incident de sécurité avéré :

- arrêter l'utilisation des systèmes concernés par l'incident ;
- ne pas éteindre la ou les machines concernées par l'incident pour permettre de sauvegarder les données en mémoire pour investigation ;
- isoler ou faire isoler au plus vite les composants concernés par l'incident du réseau informatique après accord par un supérieur hiérarchique ou à défaut, à la discrétion de l'intervenant si les supérieurs sont inaccessibles ;
- limiter l'extension possible du sinistre ;
- sauvegarder, dans la mesure du possible, le système pour garder l'existence et la preuve de traces éventuelles ;
- essayer de ne pas détruire des traces susceptibles de permettre de remonter à la source ou à l'auteur à l'origine de l'incident ;
- prévenir au plus vite un supérieur hiérarchique et le Responsable de la Sécurité des Systèmes d'Information.

5.2.2.Protection des droits d'accès à privilèges

Toute action d'administration et d'exploitation sur les ressources des Systèmes d'Information peut faire l'objet d'une journalisation permettant leur imputabilité. Ainsi, pour garantir une traçabilité adéquate, l'Administrateur veille à la protection des droits d'accès privilégiés liés à sa fonction et au respect des règles de sécurité pour protéger l'utilisation des comptes qui lui ont été confiés :

- il assure la protection des postes de travail à partir desquels il exerce ses fonctions ainsi qu'à la gestion des identifiants et des secrets d'authentification des comptes à privilèges. En particulier, il veille à ce que les mots de passe utilisés pour les opérations d'administration et d'exploitation soient robustes et changés régulièrement, conformément à la Politique de Sécurité des Systèmes d'Information ;
- il ne cède ni ne transfère ses comptes personnels d'administration (identifiants et mots de passe) sauf en cas de contraintes de service limitées dans le temps. Dans ce cas, le partage doit être opéré exclusivement par l'application «https://secret.sisbaa.fr » ;
- il n'utilise les comptes à privilèges que pour les activités et besoins directement liés aux tâches d'administration ou d'exploitation dont il a la responsabilité ;
- il utilise impérativement son compte utilisateur standard (sans privilèges) pour toutes les tâches qui ne sont pas directement liées aux actions d'administration ou d'exploitation des ressources ;
- il proscrit l'utilisation de comptes génériques à privilèges et, si cela n'est pas possible, il documente cet écart en adressant une demande de dérogation au Responsable de la Sécurité des Systèmes d'Information afin qu'un plan d'actions puisse être mis en place pour y remédier.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

5.2.3.Utilisation des logiciels et équipements spécifiques

Dans le cadre de la conduite de sa mission, l'Administrateur peut être amené à utiliser des logiciels spécifiques pour la gestion et l'administration des ressources des Systèmes d'Information sous sa responsabilité. Toute installation de logiciel spécifique doit faire l'objet d'une autorisation préalable et expresse du supérieur hiérarchique ou donneur d'ordre ainsi que du Responsable de la Sécurité des Systèmes d'Information.

L'administrateur est informé que certains logiciels, notamment gratuits, peuvent être piégés, par exemple avec des portes dérobées, et compromettre l'intégralité des Systèmes d'Information s'ils sont installés. L'administrateur ne doit pas utiliser ses droits d'administrateur pour installer un logiciel non standard sans autorisation préalable.

L'Administrateur s'interdit l'utilisation de logiciels ou d'équipements personnels pour réaliser ses actions d'administration/exploitation, et s'assure que la collectivité dispose bien des droits d'usage et de licences des logiciels spécifiques utilisés.

5.2.4.Continuité d'activité

L'Administrateur documente ses actions et interventions de telle sorte que la collectivité ne soit pas dans un état de dépendance en cas de départ ou d'absence prolongée.

5.2.5.Départ de l'administrateur

Dans un délai raisonnable suite à la notification de son départ ou d'un changement de poste, l'administrateur rapporte à son responsable hiérarchique les comptes d'administration des applications ou équipements non liés au domaine afin qu'à son départ il puisse organiser leurs modifications ou résiliations.

Envoyé en préfecture le 18/11/2026
Reçu en préfecture le 18/11/2026
Publié le
ID : 022-212202154-20261110-DB20261105-DE

5.3.Principes liés aux activités de contrôle

Dans le cadre de ses activités de contrôle qu'il réalise sur les ressources des Systèmes d'Information, l'Administrateur s'engage à respecter les principes de proportionnalité, de transparence et de loyauté.

5.3.1.Principe de proportionnalité

Les contrôles effectués par l'Administrateur, dans le cadre de sa fonction, doivent toujours être proportionnels au but recherché. Ainsi, il appartient à l'Administrateur d'utiliser les moyens strictement nécessaires pour remplir ses missions sans aller au-delà. Il s'agit par exemple de ne pas procéder au contrôle systématique du contenu de tous les messages échangés par les utilisateurs ou par un utilisateur en particulier. En revanche, rien n'empêche l'Administrateur de contrôler le nombre, l'origine ou le destinataire ainsi que le volume et le type de fichiers attachés des messages émis et reçus par les utilisateurs.

5.3.2.Principe de transparence

Les opérations de surveillance ou d'investigation mises en place par l'Administrateur dans le cadre de l'accomplissement de sa mission (sécurité et bon fonctionnement des Systèmes d'Information) doivent respecter les procédures définies et validées par sa Direction ou la Direction Mutualisée des Systèmes d'Information.

Par ailleurs, il est rappelé que le Délégué à la Protection des Données doit être consulté préalablement à la mise en œuvre de dispositifs de contrôle de l'activité des utilisateurs constituant un traitement automatisé de données à caractère personnel.

5.3.3.Principe de loyauté

L'Administrateur réalise les contrôles dans le strict cadre de ses fonctions. Son action ne découle jamais de l'intérêt personnel, mais d'une nécessité justifiée par des impératifs de bon fonctionnement ou de sécurité des Systèmes d'Information.